SM77 | 7.9.2022
Summer Playlist | Episode 2
Michelle Dennedy, CEO, PrivacyCode, Inc.

We are diving right into the deep end this weekend with former SmarterMarkets™ host and PrivacyCode CEO, Michelle Dennedy. We'll be discussing protecting our privacy in the aftermath of the US Supreme Court overturning Roe vs Wade, building a better global information economy, and what Gen X can teach Gen Z, or vice versa.
In the second installment of our Summer Playlist, Michelle and David explore how to build data systems that remain resilient in a time of extreme uncertainty — and the opportunity for self sovereign identity as we navigate increasingly high levels of physical, legal, and financial risk.

Michelle Dennedy (01s):
This is a time to build because you know, this uncertainty is like any other market condition. There will be uncertainty that is a certainty. We will not have a solid set of rules for the US anytime soon. So look to your systems and harden what you can and create the data trails that you must and delete your data as quickly as you can, where you can.

Announcer (25s):
Welcome to Smarter Markets, 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 antidote?

David Greely (50s):
Welcome back to our Smarter Markets summer playlist, where we're sitting down with our special guests midway through this momentous year in markets to talk about where we are and where we might be, and need to be heading next it's beach reading in a podcast. I'm Dave Greely, Chief Economist at Abaxx Technologies. Our guest today is Michelle Dennedy, CEO of Privacy Code. We'll be discussing, protecting our privacy building a better information economy and what gen X can teach gen Z or vice versa. Hello, Michelle. Welcome back to Smarter Markets.

Michelle Dennedy (01m 20s):
Thank you. It's great to be back during your summer reading series.

David Greely (01m 24s):
We're really glad to have you back with us today. I've always enjoyed your episodes as both a host and a guest on Smarter Markets because you make these issues, these complex issues of privacy and data security, so accessible, and there's a lot to talk about today.

Michelle Dennedy (01m 40s):
Always lots to talk about, so thank you very much and, and thanks for keeping the topic alive.

David Greely (01m 46s):
Absolutely and I think we have to begin with the US Supreme Court overturning Roe versus Wade and Justice Clarence Thomas opening the door to further rolling back the Court's established position on the right to privacy. This has so many implications and you're a lawyer and a privacy expert, so you're the person who's perfect to speak with about this. Where do we even begin to think about the implications of this move by the court on the right to privacy?

Michelle Dennedy (02m 16s):
Oh, Lordy, Lordy, I'm feeling 140 David, I think let's leave politics out of this for a minute, if you can, because depending on what time of day you're listening to the pod, I am not sure how strong a drink you can make to get through this timeline. So let's approach this first from the legal perspective, the grasp from Griswold Casey and Roe, the progeny of healthcare data and data privacy at the Supreme Court was always a bit of a tenuous sort of ban together. So for the last 50 years, we've sort of been winking and nodding at one another saying the informational right of a patient to have a sacred conversation with her doctor and his doctor, because we are talking

about family planning and reproductive rights and not just the uterus. We're talking about both pieces of the equation here. So both the fertilized and the fertilizer in the past for the past half century have had the right to privacy codified in case law and decision making that the Supreme Court formerly was validating saying that you should be able as part of your right as a citizen inherently as a citizen of the United States, you should have the right to have certain types of conversations and intimacies that fall into this category of privacy.

Michelle Dennedy (03m 46s):
And some of it is personal privacy and physical privacy and integrity. So the right to be left alone, this goes back into jurisprudence and traditional US fashion into the 1890s with the famous Warren and Brandis, right to privacy article that was in the Harvard law review and so when you think about not just the right to a certain type of healthcare for women, think about it more broadly of can you ask your doctor for a certain type of hormonal adjustment. So whether you're taking these types of hormone adjustments, because you've got acne, or you would like to delay your body from hormonally being prepared to have a child, or you are in menopause and you want to prolong your health and wellbeing, all of those various conversations fall into different context buckets that are now very much in question. So there's sort of two things that are, are falling out apart from reproductive rights and, you know, equal protection rights under the constitution, which are all in big question and big format, I just want to focus for a smarter market on what does it mean to have a class of data that we assumed enjoyed 50 states worth of protection i.e. health data that now has a very big question.

Michelle Dennedy (05m 02s):
Does that data enjoy protection as an inherent right, you know, to life liberty in the pursuit of happiness, or is this something that is more of a commercial, right or a segmentable or an alienable right that should be outside of the realm of something that we all have as human beings who exist on, you know, in this country together as in a federated democracy and so various, like you can vote or you can vote not to have these sort of rights. So what are the implications here, when we think about health apps, not all of these devices are collecting information to provide that information to your doctor or some covered entity to provide you healthcare. So they may or may not fall under the federal HIPAA, which is the health insurance portability. There's no privacy in HIPAA, but there's a very strong security and privacy rule in HIPAA. Does HIPAA even stand if there is not a federally constitutional protected right to privacy. We don't know, so that's a very long winded and we could, I could go on with a lot of wind that would make a tornado, but the implications of Roe are not abortion. The implications of Roe are data, data privacy and individual freedom to make determinative and have conversations that do not have government involvement.

David Greely (06m 32s):
Right and it's so important that the conversations with the doctor as said, we're always considered sacred and now it's unclear of, you know, can the police or an investigator come in and take those conversations and what's the chilling impact on having a honest discussion with your doctor, you know, wanted to get into like the technological piece that you brought up because so many of us are using these health tracking apps, many women track their cycles using these types of apps. I imagine there are some ways just through, you know, things like apple watches and other fitness trackers that you could determine, you know, where someone is in their cycle and does everyone have to be much more cognizant about the data that's being collected and is there any security around it at all this point, other than, you know, what can technologically be put to lock it down?

Michelle Dennedy (07m 25s):
Well, I think these are two very huge thoughts, I think and let's, let's start by digging in with security and privacy. What is that relationship of one to the other where private data must be secured and secured over time, in context and free from outsiders, observation and disruption and corruption. That's the security piece. Privacy is much broader than security. So talking about, are you allowed to observe the conversation is a one-to-one conversation between patient and doctor. Am I being a patient when I'm talking to my next door neighbor who happens to be a doctor probably not. It's similar to, am I being a client when I talk to my neighbor who happens to be a lawyer, now I, my lawyer by training, I often say this is a legal opinion I might have. I am not your lawyer. We're very clear to say that.

Michelle Dennedy (08m 23s):
And often doctors will say the same, because there are very real responsibilities and fiduciary duties when that relationship attaches. Now, the assumption on the person who's sharing matters here, right. So thing, number one is security is not privacy. So even if something is secure, it may not be private, it may not be controlled with your consent, according to context, it may be shared in a way that you don't expect, or you find to be disrespectful or even harmful. So understanding technologically locking things down, quote unquote is a tremendously hard to do. The security industry is mostly reasonable efforts based and also where we don't really

understand what the privacy engineering requirements are. So who has the life cycle fiduciary care for that data that's coming in through your watch from your skin into the sensor or is it coming in through a camera, is it your camera are we working out together, Dave and I go for a jog and I happen to be recording with, you know, whatever the, the newest version of Google glass, if you're old enough to remember that when I'm observing other people, all of these data elements. So even if a woman decides not to track her monthly cycles, if she is sharing a home with more than one woman, it's very likely you can guess what her cycle is. If other people are tracking theirs, you know, fun fact we often align with our hormonal conversations that we're having in thin air. So understanding the implications of what are data analytics, what are you allowed to have, what are we giving away and what are we accidentally sharing. What does all of this mean for privacy engineering and what are our responsibilities as community members, as family members, as parents, as employers, and as people in general societies who may be even standing on the border of maybe one state has state laws that say one thing about that information and its privacy and another state might have different rules and yet the IT infrastructure underneath it only recognizes electrons and not electrons. So we have to really think about what does this means for how are we building our systems going forward so that they are resilient in a time of extreme uncertainty and extreme physical safety, legal, and financial risk. Isn't this supposed to be a summer beach re David, my goodness, we've gone dark.

David Greely (11m 01s):
I feel like privacy and security conversations have a tendency to do that. At least

Michelle Dennedy (11m 06s):
We kind of love it. I'm not gonna lie.

David Greely (11m 08s):
Yeah. Well, it's, it's a bit, it, it's just so fascinating and I, you know, as, as a man who will never be pregnant, it's also interesting to think

Michelle Dennedy (11m 15s):
It's early days, David it's early days.

David Greely (11m 18s):
Technology's always advancing by that way. I feel like I'm done. It does raise the interesting question of does someone like myself have a different level of privacy in conversations with doctors because no one will be looking to see if I'm pregnant and then not pregnant, and what happened in between and what does that mean for like the idea of equal justice under law, I have a different expectation of privacy than you would?

Michelle Dennedy (11m 47s):
Right well, and if you're capable of fertilizing someone else's egg and we do have the science that we didn't have in the 1960s that says we can look at your DNA. So every baby born or every fetus created, whether they're born or not we can look at the information that is encoded in each of the cells and we could say, this person has a 99% chance of being fathered by, you know, person X and mothered by person Y. So if we are doing an equal protection under the law under today's contextual scientific capabilities and the information science tools that we have available, one would say that the death of data privacy at, you know, as a fundamental human right, as a basic construct of a free society rather than a state by state sort of commercial, you know, trading card, you have to really take another step backwards and say anyone who is capable of creating a blast assess, or a zygote, do we now register everybody's DNA?

Michelle Dennedy (12m 55s):
Do we require vasectomies that are easily reversible, but are pretty far up the supply chain, as it turns out in the fertilization game, and we're not talking about abstinence anymore, we're talking about disrupting the supply chain. What are the implications here outside of and I know it sounds kind of sort of monstrous and I'm not trying to again be political, but I'm looking at it from a data perspective, a legal perspective of how do you now apply today's science and what we know about the ability for us to freely travel quickly travel and the transactional nature of fertilization versus the state over time of, you know, a being pregnant. So I can be fertilized in Texas and I can be pregnant in California and that that's two different implications, but the transaction probably happened somewhere one place or another.

Michelle Dennedy (13m 54s):
So where do we apply the law, where do we apply the consequences and how long do these data implications get stored and by whom, so that's as a data science person, as a market watcher, as someone who's predicting privacy engineering requirements, you know,

right now we're asking our employers in the US to supply our healthcare. If our healthcare is tied to the ability to support a blast assess fetus baby, does that mean everybody has to come with some sort of a child birth child care insurance policy. Are we asking our employers now to proactively either require that you're doing something about your reproductive world or are we saying, because you're already burdened with healthcare now you should be burdened with information monitoring of these humans that tend to sometimes create more humans and you can see how this gets more and more monstrous as you play this out as a systems engineer, because it, it gets you to a very absurd place pretty quickly where you really want to pull back into the marketplace again and go, okay.

Michelle Dennedy (15m 11s):
It turns out that individual self-sovereignty is a pretty cool thing, both because I don't know, it's kind of fun to feel like we have our own free will, but also from a systems engineering perspective, it's good to have a start middle and finish of relationships, either as an employer, as a citizen, as a child, as a student, these are things that we understand in situate and systems and I sort of leave the spiritual to the spiritual people and I leave the transactional and the data interrogation and even data justice to systems and systems engineers.

David Greely (15m 47s):
And it certainly seems like the, Pandora's Box has been opened here in terms of implications of this and, you know, we are Smarter Markets, so we're focused on self-sovereign identity. We're focused on market issues. There is so many important things about, you know, basic human rights, but that's beyond, beyond what we can really get into here.

Michelle Dennedy (16m 07s):
For our market builders, you want to build, right. This is a time to build because you know, there, this uncertainty is like any other market condition. There will be uncertainty that is a certainty. We will not have a solid set of rules for the US anytime soon, so look to your systems and harden what you can and create the data trails that you must and delete your data as quickly as you can, where you can.

David Greely (16m 35s):
And, and I wanted to ask you about the economic implications for the United States. Uncertainty is typically not good for economies and investment and markets and, you know, there was a recent event where Italy's data protection authority effectively banned the use of one of the audience measurements tools in Google analytics as it's not compliant with the EU Data Protection Regulations, because it sends data back to the US, and the Italians ruled that the US safeguards on that data, weren't adequate to European levels. So that's like if someone in the United States think we're one of the leading you know, information is what we do technology is what we do and now other countries aren't allowing analytics to be used because we're not secure enough. Can you explain what's happening in Europe and what it means now that you know, US Data Protection will likely be even less adequate than at the time of this ruling?

Michelle Dennedy (17m 39s):
Yeah. So I mean, explaining the vagaries of data protection law in Europe is about as easy as explaining what the heck is going on the Supreme Court bench these days.

David Greely (17m 55s):
So we only give you the easy questions Michelle

Michelle Dennedy (17m 58s):
Yeah, we'll give it a step. So I, I think it's really interesting because at the turn of the last century, I would've told you that by the year 2022-2023, we would really have embraced data treaties. We would've recognized that because we do like to draw revenue from other countries. We like to have families that rather hither and yon based on our current technology, and now with, you know, the ability to do video and voice at a very cheap level, you know, when I was coming up a long distance phone call was like a dollar a minute or something, and you'd call your mom collect and say, it's Henry calling.

Michelle Dennedy (18m 36s):
And she'd say, I don't know any Henry, and that would be your signal and she'd hang up. Now we transact business seamlessly across borders so at the turn of the last century, I assumed that this is where we would be going and therefore, economically, socially, commercially, we would have these data treaties where we would have a certain level of security that we would agree to. We would figure out, you know, what is that, what we used to call a web tone at Sun Microsystems, where you'd have a certain availability of

processing power. Those things have not happened as it turned out and so when we first started putting geographic borders in place for data and started saying, you know, one country could reach out or one region in the European Union's case could reach out into another region and say, you are not adequate.

Michelle Dennedy (19m 27s):
And therefore the default position is, do not share with countries that are not adequate and adequacy here for what we're talking about for Google analytics or other analytics too. I don't want to call out one company because that's not the point, the ability of any private company in the United States to resist the US government from asking, using, you know, under current law, let's leave the crooks out of this, let's leave the cyber criminals and then the hackers out of this for a minute using legal process that is the state of the state. If a private entity in the United States is subject to that kind of interrogation and has that kind of data accessible to it under this kind of an analysis from Europe, they're saying that any sort of data that has personal data or personally identifiable data, which has very broadly defined can be an IP address, can be a grid from your phone or your device.

Michelle Dennedy (20m 31s):
It doesn't have to be your name and actual, you know, birth certificate or social tax number, but if you have any information about Europeans or that describes Europeans, and that's capable of being asked for under process from the US government, then that can be deemed unlawful data and therefore there can be a blockage of that data from traveling now in a world in the market where data is currency and I'm not talking about selling data broker stuff or even the advertising business, or even the analytics that Google is currently the case under the Italian case was Google analytics. I'm talking about actually knowing things about employees or customers or future employees or customers or citizens that is the currency de jure in an information based society as we have. So we're talking about one region being able to stop that processing to cut off any revenue or innovation based on that currency, traveling from border to border just this morning, there was a case in Ireland that was decided against Facebook.

Michelle Dennedy (21m 45s):
That basically said they found that the transfer of information on Facebook to the United States about European citizens was unlawful and because the Schrems two decision came down and said that the privacy shield was no longer valid so agreement between the US commerce department and the European Union no longer valid because the US government can under lawful process ask for information. They can't use that vehicle. So Facebook did what everybody else did and they used what's called standard contractual clauses. They did a whole bunch of different legal agreements, those failed for the same reason and fundamentally a year from now, when all of the rest of the European Union chimes in and says, what do you think what they can't do and what is not under a private company's control is will there be this agreement where the US government will not ask private citizens and corporations who unfortunately under citizens United, which is a whole another problem.

Michelle Dennedy (22m 53s):
When you think about that as a person, and it's a person that lives everywhere until that agreement is made and strengthened and deemed adequate, we are going to have these constant barriers in trading and so what happens in your marketplace is you have to build data centers locally and so only the big players, ironically, they think they're democratizing data and they think they're democratizing competitive value and what's happening is the big players do have the capital to invest in local data centers and the little guys do not. So will there be luga gao will there be La Facebook Elvira Visser, maybe, but probably not. So we're either gonna have to figure out how do we work as privacy engineers to have even more clean snippets of data that is provably not associated with an individual, or we have to build and do real estate infrastructure and a, big focus of this podcast is how do we fuel all of this with energy, so that we're basically enervating social networks and, and other types of utilities based on data that actually can operate lawfully. So again, like long answer I'm like long-winded today, David, I don't know what's up

David Greely (24m 15s):
I'm glad because I'm just taking it in and well, it's amazing, right, where we think of, you know, you think of data as being so fluid, fast moving crosses borders, you know, the ultimate international good and it seems like we're, we're introducing all of the barriers to trade that we're so used to in the material world, you know, are we gonna have barriers to entry. Are we gonna have trade wars when it comes to data. Are we gonna need a WTO of data at some point?

Michelle Dennedy (24m 44s):
I think we will. And it's kind of up, it's kind of upsetting because this is when the slide rule brigade should really be at our best. Like this is the time for math. You know, like data is, is ultimately an electron that's getting pushed, hither and yon and so having rules of

engagement, shouldn't limit information, having agreements and what I call the surveillance economy, where you have a few bad actors in particular that are hell bent on observing everything everywhere and they've convinced themselves that this is somehow ethical or moral or that somehow we've agreed to it because we're willing to take a picture and put it on a social network or were willing to come to work and therefore you get to spy on me through my camera, in my home office, all of these myths about how people actually operate and how morality should, and shouldn't be put into the investment vehicle that, that I think probably comes up through ESG at board level. I think there's a lot of innovation to happen in board reporting. There's a lot of innovation that has to happen at the SEC to say, what is a good company, what is a company worthy of investment and it's not how much surveillance can you get done and how much data about someone else can you sell?

David Greely (26m 03s):
Yeah and, you know, sadly, we've all gotten to accustomed to giving up our privacy to the big companies like Google, Facebook, Amazon, because you really have to, if you want to be part of society and the economy these days, it's hard to think about operating without it, or, well, well, what else can I do so?

Michelle Dennedy (26m 20s):
Fast, not so fast young man. I don't think we have to and I think that there are some bad actors in that bunch in the Fang gang, if you will, that have convinced a slice of us, that that is true. So if you want to converse with your elderly aunt who is on a certain platform, you must quote unquote, give up your privacy. I think thing number one why should I. Right now I don't have a lot of competition and so I do it, but I don't like it and the reality is, if you ask that same question of the Irish immigrants, my people who came to New York city at the turn of the last century, you know, going from the 1800s into the 1900s and you looked at it economically, you would say, wow, those poor Catholic people love eating rat and saw dust.

Michelle Dennedy (27m 15s):
Like they, we make sausages out of rats and the worst part of the beef and saw dust and sometimes we pour some bleach on it so it doesn't stink so bad and man o man o shove, it's those Irish people, they eat that up. If you looked at the economic flow, you would say, wow, same, same thing. Like those Irish people sure like them rats. The reality is when, when Upton Sinclair revealed what was going on in Chicago and New York and the abattoirs and the fact that there was no food, safety regulation and people were allowed to hide and lie and fill things that go into people's bodies and they feed to their children with these horrible poisonous substances, they had to buy it because it was literally the only food available, but they certainly were not choosing to eat things that were unwholesome. I think we'd been eating a whole lot of rat and it's and I'm kind of over it and I think there's a lot, we can do it about it.

David Greely (28m 18s):
I'm optimistic about that. I'm glad to hear that. You've kind of put me off hot dogs for the summer though.

Michelle Dennedy (28m 23s):
I know it's a summer read. I know. Well, hot dogs are regulated. You know, you have to have only wholesome parts in your hotdogs.

David Greely (28m 31s):
And I also wanted to ask you because you know, but in order to get to that better place, we kind of all have to band together, right, yeah. It wasn't private acts that changed the Chicago Stock Yards and the meat processing industry. It was people like Sinclair kind of galvanizing public attention and then people demanding that, you know, the right to quality food and you know, regulated food was handled by the government and you had, you know, the U S D a and everything else. So what would the equivalent of that be in this moment, do you think?

Michelle Dennedy (29m 05s):
Yeah, I think there are activists amongst us that are kind of the repertoires, you know, we've had some great you know, Kashmir hill and Julia I'm gonna say her name, wrong angular. Who've done some revelations about like what these social networks know about us, et cetera. So we have people talking about it. We have the EFF, we have the ACLU, then we have this sort of crop of innovators and I'm really proud to work amongst them. So my company is called Privacy Code and basically it's based on the premise that while I've been talking to and talking about and writing about, and even wrote a book about privacy and privacy engineering for the last 25 years, the shame of it is people don't tend to take the privacy engineers manifesto to the beach with them and consume it and go, I'm gonna change my world.

Michelle Dennedy (30m 00s):
I am a privacy engineer. There are some people that have done it. The reality is if I can convert something really complicated into something that you can do in two weeks, or you can do in a sprint or you can plan, or you can mark, or you can prove then one by one you don't have to be a subject matter expert in privacy, but you can have an identification vehicle where you're doing using a self-sovereign identity technique to not overshare and you can, if you're consuming information, you can make sure before you're putting together some sort of machine learning, you can actually check the provenance of the types of data that you're buying. Are you buying rat data. How old is that data and if you start asking, whoever's selling you the data, how old it is and not just is this consent covered data, which is always been garbage data.

Michelle Dennedy (31m 01s):
Where did you get this data, what was the context, how old is it and we start consuming these ingredients. We're gonna get to what I call organic analytics like that delicious strawberry. That's just the right flavor and just the right time and you're, you're putting it on your plate and you're slicing it up and it's almost decorative. It's so beautiful you don't want eat it. That's the kind of analytic that should be the thing that you're talking about at your board. Like we're using the best data and we're getting the best insights and we're measuring it and our customers are actually delighted about it. They're not sharing this picture because they have to, they're sharing this picture because it's them delighted to be personal and get real with us. Or it's a woman who is trusting you with her health information, because she has to do something about this terrible pain she's having and she doesn't want to be castigated as if she's doing something naughty or wrong because you've proven yourself worthy. So you've curated your data. You've gone beyond security to keep bad guys out and you've proven yourself worthy. Otherwise these other people are going to eat like these little, you know, gelatin like pink things that we're calling strawberry jam, but I want you to have organic data. David.

David Greely (32m 23s):
I would like that too and you're making me think of, you know, on this podcast, we spend a lot of time on the ESG and thinking of things like the voluntary carbon markets, where government policy not moving fast enough to address an important issue in that case climate change. So you've got stakeholders, activists encouraging corporates to make net zero commitments, and then, you know, holding them accountable to that, it sounds like you're saying we might experience or, or that would be another avenue to get more privacy. If the, the corporations that are the buyers of the analytics based on our data are held to account to be okay, we want you to be, you know, what is your policy on protecting the digital privacy of the people who you're buying analytics based on their data, are there certain standards in place and then we'll hold the, the boards accountable. Is that absolutely. Is that one pathway that you're thinking of?

Michelle Dennedy (33m 17s):
Absolutely. I mean, what you know, again, this is my little company it's called Privacy Code. If you have done all of the elements of privacy engineering, you should be able to prove them. You're already doing it. Now, you're going into your sprints and you're asking people to do two week proofs that they're doing proof of work at the end of all of that work, you should have proof that it's done. We're already doing quality testing before it goes out the door we're doing collections of P1s of the most, you know, dire security risks. We sure as heck should be doing the P1s for privacy, where we're saying, hey, this feels icky. Or this seems like too much data collected for purpose or wait a minute. There's no expiration data on this. Yuck. That's not something that's gonna be delicious.

Michelle Dennedy (34:07):
That's not organic data. So when we're looking for those aspects and we actually roll all those things up, do you have a quality program. Have you appointed a privacy officer who is not a compliance person of course, you're doing compliance that's the basic that's like showing up in the morning, but are you a privacy strategy person, are you talking about the nutrition of your data, are you strategically ready to go to Europe. It's not just, are you getting away with it because you've always gotten away with it because things are getting hot over in Europe. They're building a very big digital wall over in Europe. So are you ready to scale that wall as senior leadership and the only way you get in around under and through that wall is to build a contextual consent economy versus the surveillance economy and the companies that are gonna win and the companies that are gonna be resilient are gonna build that in from the board all the way down to the bottom.

David Greely (35m 03s):
And getting that the, the SG into the ESG.

Michelle Dennedy (35m 06s):
That's right.

David Greely (35m 07s):
And as you said, with Europe, building more of a wall, it also just becomes a pure profit business, are you gonna cut out a large market from your, from your company?

Michelle Dennedy (35m 17s):
And don't think it's just Europe, because guess what China's belt in road already has agreements in place. China has very strong privacy law. Their concept of privacy is far more communal and I don't mean communism. I mean, communal they have a different societal approach philosophically to groups of data and designation of origin and family ancestry and time than we do. Hong Kong has always had some of the strongest laws. Singapore has strong laws, Latin America has something called habeas data where the data should be staying in Brazil under LGBD. These people have very strong points of view on what should your system look like, these are systems ingredients, are you ready to be a global player in the information society, get ready it's common.

David Greely (36m 12s):
Well, I want to shift gears for a second and go to the point of view of a parent. You know, it's the summer that kids are out of school, as our conversation is probably suggested I'm from generation X and I realize like we're the last generation to come into a world without personal computers, smartphones in the internet, and then have them all arrive while we're here. I mean, I remember the learning to program. We didn't call it coding back then on a Commodor 64 and walking down to the computer lab in college to check email. Yep. I mean, that's all those ridiculous things. It's like being in a horse and buggy, but I see my gen Z children growing up in a world that, you know, has pretty little regard for their privacy and little expectation of digital privacy and I'm curious, like, how do you see that generation that's kind of grown up in this world of very little privacy dealing with that lack of privacy and is there something that we can do those of us with memories of it to help them rebuild a culture of privacy or is it going back to the horse and buggy?

Michelle Dennedy (37m 18s):
No and I actually think, I think privacy needs, I think we need a marketing rep, you know, when Steve Jobs said cloud, suddenly having utility computing seemed like a possible and feasible business. You know, when we called it the grid or the utility, when I was at Sun Microsystems, everyone was like, yon, yon that's those geeks talking again, suddenly jobs comes out and calls it the cloud and we're talking about weather and rain and sunshine it's the same darn thing. It's a server. That's not yours, but the thought of not having to buy a rack and have your cords managed and have your HVAC paid for and real estate decisions made before you can even have capabilities changed everything. So I think when we look at privacy, as we looked at cloud, if we had a better word, that's not security.

Michelle Dennedy (38m 14s):
And the notion of privacy I think is probably led best by what I think of as a student council. So think about the digital natives and, and particularly gen Z I have two gen Zers. They're both, you know, my daughters are five years apart. So one's a little older and had a later entree and is very irritated that my younger daughter got her phone much earlier and I was much more permissive with the second one and, you know, things had progressed. I think if you look at their behavior in an anthropological kind of sense, and you see what our kids are actually doing and I say kids like my, my oldest is a young adult. There are different personas that they self-select, some are selected for them because they're on a cheer squad or they're in a sports team and so their coach says, use this app.

Michelle Dennedy (39m 04s):
You must, some of them are, you have to be on this platform to be educated during a pandemic, but the things that they choose for themselves, the, the way that they entertain themselves, the way that they educate themselves about the issues, the way that they interact with communities that they care about. I didn't have friends in Iceland when I was 12. They do, I didn't have a persona that was like, you know, this cool punky little fashionista that my one has, or this like, you know, rabid protest, eco warrior chick that my other one has, but both of them have the Sunday school for grandma persona things. They both have Facebook accounts. I don't know who those kids are on Facebook. They are not my children. They're these perfect. I got an a, today. I graduated, I disappear until Easter and then I'm back. So if we, if we had, if my employees at these big companies that I used to work for all behaved like my 13 year old girls, when they both were 13 with the secret of who is your crush, if every employee only was as secure as a 13 year old child, with the information of who is your crush, we would not need a CISO.

Michelle Dennedy (40m 26s):
We probably would need a lot less technology. You cannot get that information from them under torture. You cannot get that information. So thing, number one, they know how to keep a secret where they want to keep a secret thing. Number two, your secrets, aren't their secrets. So just the fact that they're always doing stuff that you think of in your wisdom as risky, it's just not risky to them. They don't have your wisdom and understanding that they unlike us switch platforms like they're changing t-shirts on and on and if you don't please me and you don't respect my personal space, they may not call it privacy, but they will switch and they will leave you and that's the difference. I think that, so this generation coming up absolutely understands platform. They understand community, they have a much greater expectation of globalization and that's not just coming from a Western point of view, like working with children from other parts of the world that have access.

Michelle Dennedy (41m 23s):
They do. Now, the other big part of this is there are a huge, huge, you know, billion cadres, strong and 65 million people this year alone who have been displaced by war or climate who have no access. So we're talking about a very big world of, of have and have not, but where the world is connected and we are largely connected. We have a different expectation of civic duty. We have a different sort of, how do we behave online, we haven't set the rules yet on manners. I'd like to see better manners when you're anonymous. I'd like to see that, but I don't think that's a lack of privacy. I think it's just early days. I think there weren't a lot of manners in San Francisco in 1849.

David Greely (42m 08s):
Well, you've given me some hope that the younger generation, maybe a step ahead of figuring out how to, to recreate some privacy for themselves, at least and I often realize that, you know, with many things in life once we lose it, we realize how important it actually was to us and then we start to work hard to take it back. Even though we often have to work harder to take it back then we would've had to work to keep it in the first place and with the developments we've been talking about today, I hear a lot of people who want to call to action, but what can we do and where do we draw hope from and, you know, we talked a little bit about where we can start, but I was wondering if you had any other hopeful thoughts on where we could start today?

Michelle Dennedy (42m 48s):
Yeah, I think, I think we need to, I think we need to demand more. So regardless of where you are, whether you're a technologist who needs to demand more clarity on what are privacy and security requirements, you are a board member. You need to demand more information about how are we going to be strategic in an information society. Why am I only hearing about cybercrime, why am I not hearing about data equity, why am I not hearing about data provenance, where are measurements relating to the availability and portability of data sources to growth as an investor I want to see that. As a venture capital community, why do we still have these dinosaurs out there saying don't build privacy in and don't build security until the end I'm like, I used to be the buyer like right now, I'm a builder and I am pen testing myself from the first line of code that we've written granted, I'm a security and privacy person.

Michelle Dennedy (43m 46s):
So of course I'm gonna do that. However, I've also been a buyer for most of my 30 year career, and I have either taken huge multimillion dollars and put it in escrow for, during the deal closing for the cleanup, because a lot of times your red flag isn't big enough as a privacy person to kill a deal, but I guarantee you I'm taking that chunk and I'm giving it either to the PWCs or Deloittes or whomever is helping me do the cleanup on I L six, or I'm keeping that back to either pay bad debts of privacy, billed more security or in some cases. So when WhatsApp was purchased by Facebook, I'm not an insider on either of those deals. This is just the Goss going down, Silicon valley, not a single line of code of that original thing ended up in the real thing. So even though they already overpaid $2 billion for something. Now they got a lot out of it.

Michelle Dennedy (44m 52s):
They really overpaid because they had to rewrite the whole thing. So had they been following the rules and had they been doing the right thing from day one, you would've had more pure profitability and we're gonna see that more and more and more as you're talking about SAAS services, as you're talking about healthcare apps, as you're talking about more and more covered entities falling into these buckets of regulated CCPA, CPA state law and internationally influenced stuff. So regardless of where you are in that spectrum, demand more ask for more information. If you're a builder built, if you're a security person, make sure you understand the corpus of which you are securing. If you are an observer, because you think you're gonna sell data later, understand the context and put a data on that thing because that strawberry is going bad. Fast.

David Greely (45m 47s):
Thank you for all of that. Give me a whole lot to think about and some hope for the future and actionable steps, like things that we can actually be doing to improve the world and improve our markets and because this is our summer playlist, which I think of as our beach reading and a podcast, I'm also asking everyone, and I'll ask you for one more thing, which is what's on your personal beach reading list this summer.

Michelle Dennedy (46m 16s):
Okay. I'm gonna cheat. I warned you in advance. I was gonna cheat.

David Greely (46m 15s):
You, you have a dispensation.

Michelle Dennedy (46m 19s):
Okay. Thank you. It's kind of an add thing. I think. So I'm reading two books right now. I'm rereading atomic habits.

David Greely (46m 25s):
It's great book

Michelle Dennedy (46m 25s):
Because yeah and everything we talked about today is like, I guess I'm an incrementalist and always have been, but like you said, like we, we do bad things and then we pay for them. Well, I put on £30 during the pandemic, it was a lot more fun and easy putting that on than it is taking it off and the only way to do it is like one little thing at a time, one little chunk, like the world seems really hard and really big and really scary right now and guess what, it's no scary than it was in 1933 or in 1945 or 1966. So we can do this Atomic Habits personally, globally, socially. So that's like my like kind of gives me hope and like remind myself that this is all doable, but and then the other one is a pure beach read Page Turner Cops and Robbers, former cop turned detective called Be Gone by my dear friend, Dennis Fisher, who used to be a journalist and now he is a novelist and a journalist.

David Greely (47m 31s):
Well, that sounds like some good beach reading, good escapism but like you said, you're cheating you're also doing something good for yourself. So yeah, very well balanced.

Michelle Dennedy (47m 44s):
Well, yeah. As well, balanced as a startup operator can be

David Greely (47m 46s): Well as a startup operator, who's going 24 hours a day. Thanks so much for making the time to spend a little of your summer with us. So really appreciate

Michelle Dennedy (47m 50s):
Absolutely.

David Greely (47m 52s): It was great catching up with you.

Michelle Dennedy (47m 55s):
You too. Thank you so much and thanks for this series. I have really learned a lot. Thank you so much.

David Greely (47m 58s): Thanks again to Michelle Dennedy, CEO of Privacy Code. We hope you enjoyed the episode. Join us next week as we continue our summer playlist on Smarter Markets with our next special guest, we hope you'll join us.

Announcer (48m 13s):
That concludes this week's episode of Smarter Markets by Abaxx. For episode transcripts and additional episode information, including research editorial and video content, please visit smartermarkets.media. Smarter Markets is 100% listener-driven. So please help more people discover the podcast by leaving a review on Apple Podcast, Spotify, YouTube, or your favorite podcast platform. Smarter Markets is presented for informational and entertainment purposes. Only the information presented on Smarter Markets should not be

construed as investment advice, always consultant licensed investment professional before making investment decisions. The views and opinions expressed on smarter markets are those of the participants and do not necessarily reflect those of the show's hosts or producer. Smarter Markets, 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 Smarter Markets. Thank you for listening and please join us again next week.