PRIVACY BY DESIGN IN THE INTERNET OF THINGS

EPISODE 62 PODCAST TRANSCRIPT

With me today on the IoT Show is Paul Plofchan. Paul is Vice President of Government Affairs and Chief Privacy Officer for home security company, ADT. Paul leads ADT's political engagement and public policy strategy. He's also a leader within the company's data stewardship program, focused on fostering customer and employee trust.

I met Paul a couple of times speaking and introduced him for his keynote at Internet of Things World just a couple of months back.

Paul, welcome!

So, have you been on the road lately?

Well, you know the drill in this. I have been on the road doing a lot of different things, legislative stations are taking place, Washington issues to address and then of course continued work on privacy and Internet of Things, so getting around.

You're the first Chief Privacy Officer we've had on the show. What does that entail? You've kind of indicated a little bit there but what does it entail?

In the Chief Privacy role I have the pleasure of working across the organization with my colleagues on all the different functions on how we treat customer data and how we provide the inside and thoughts into the product and services we're bringing to market and what the various privacy considerations that are involved. Also, it does sail really nicely with the work I do on government affairs because of the greater discussion that's taking place and has been taking place for a while now about various privacy issues both societal and then of course the attention that's being paid to it from an Internet of Things perspective.

Right, it's hard to keep on top 5:00 of the technology but it seems like they're now getting in the full swing on IoT. I know there have been a few documents that have been released, I guess advice documents. How would you classify the government's approach with IoT at this point in time?

I think the direction you're headed is sort of what kind of advices the government is giving in terms of B2C, business to consumer device. I think that's a good way to describe it; that could be easily understood by folks. Various governmental agencies, whether they're at the state level in terms of maybe state's attorneys generals, California attorney general for example or at the federal level with the FTC or the Department of Commerce – they've all been very involved in the space, they offer a lot of educational materials, they provide

helpful tips to consumers online. And then of course even in some of the regulatory proposals that get made, there's good information there. Even in enforcement actions, you can learn a lot about what the environment is shaping up, how people are using it, where the holes are if you will from those types of actions. But I think the government has been playing a very supportive role, they hear from consumers, policy makers, frequently get phone calls or have notes dropped to them or gets spoken to in public places about this space as it's relatively new. And then of course you mentioned being on the road, there are a lot of conferences that are taking place and I've been impressed by policy-maker and regulator outreach through that avenue as well.

Are you seeing IoT coming up in other conferences that you're attending maybe with your sector privacy? What does that landscape look like?

Certainly, I think it's occupying a lot of the agendas. In terms of privacy meetings that I attend that are strictly for privacy folks like myself I might be put on by, for example, the International Association of Privacy Professionals or IAPP. They have regular programs that educate professionals and the IoT has a very big focus not only in terms of privacy but in getting it right. I was recently at IAPP Canada and the whole focus was on the analytics aspect of big data – as we collect the data what are the best practices, the legal requirements, what are the customer trust building structures. There's that organization. I, also in my role, have the pleasure of interacting as I already mentioned with state attorney generals and they do consumer protection meetings and other types of meetings where the states are sharing ideas and there's been a really strong focus for a number of years on that. And then my role takes me onto Washington D.C.. I bet everyday these days a meeting going on in D.C. related to big data, in fact I had the pleasure last week of being in D.C. for a few days and stopping by one and I went there because one of the main talks was all about the Internet of Things and what kind of IoT good practices should be put into place. So there's lots of attention on it and it's all very helpful; it's a great way to learn, to stay fresh and contribute. I think it's a pretty robust environment. Then of course as you also mentioned where our paths have crossed at some of the inform meetings, in IoT World for example, great focus on it and a great opportunity to work with the developers and listen to them and see where they're going. I think it's all having a very positive impact.

I'm just wondering, Paul, what's your advice for the listeners? Obviously, they don't have the opportunity like you do to visit and then actually attend these meetings, maybe go to all the conferences. But do our listeners have a mechanism to influence government in privacy for example?

I think certainly they do. In the group of listeners here who are, let's just take companies that are developing products or are offering a service, they have 10:00 their own mechanisms through their own channels but I don't think you have to make it overly complex. There are just regular routine channels using constituent affairs for example into

D.C. where you could talk to that. I find legislators have a growing interest so if you're an organization and you just use your routine constituent affairs mechanisms, I think you're going to be well-received. For example, there's an effort in D.C. now, very bipartisan effort on some legislation called DIGIT Act and Internet of Things is the core of it. There's that mechanism. And then I think through regular business association member groups, your local Chambers of Commerce is all good sources. In this particular space of Internet of Things I'm just thinking of some of the companies in the Valley, there's also great mechanisms there through some of their associations, one being the Internet Society which is really, really engaged and offering some really great advice.

It sounds right. Utilizing industry bodies that your company might be part of and even I guess more horizontal bodies like the Internet Society is probably a logical way to kind of get your feelings known or at least keep on top of things?

Yeah, even just routine trade association. There's pretty much nobody today, maybe there's somebody but by large the Internet of Things and how we get this right and how we bring the most value for consumers is being talked about in so many different formats and then largely that leads into my space, which is regulatory and consumer privacy because they're topics that folks want to talk about not only for their own companies but I mean we're all users of these technologies too and we're all developing our own belief systems around how we want to use them and how we want our information to be treated and what's good ground and what's not good ground.

I'm looking forward to getting into that. Paul, give us a bit of a background about yourself and the background that you have in IoT.

I got started in my professional career on the sales and marketing side. It was after a short stint. I was a Naval officer right after college in engineering. After the Gulf War I went to work in Healthcare as the salesman and worked my way up to Marketing Sales Leadership. Within the health space, I moved to Corporate Affairs and Privacy through a legislative perspective largely into privacy. I got involved in Corporate Affairs because the government and other large organizations were becoming decision makers. And then as part of that, I got interested in privacy because of the growing concern around that. And when I came to ADT, I came to help create the government affairs department and I had the pleasure of working with the innovation team. It's part of our privacy structure maybe because my marketing and sales background or maybe because I drew the short straw, I don't know, I loved it and it was great. Short time after that I had an opportunity to move into the Chief Privacy role. Our Internet of Things connection is an extension at ADT of our traditional security products offering. As consumers wanted to incorporate other devices into what they were using to provide their own security and automate their homes, it was a natural extension and it was also a nice place for me to be involved because again, some of the policy considerations and discussions that were taking place a couple years ago in terms of

how do we transition more completely to broadband, do Edge providers need particular concerns under the national debate that was going on in Net Neutrality, has Internet of Things in the economic opportunity of Internet of Things has gotten understood or become understood, more understood I should say. That draws in a lot of interests so the whole policy maker, regulator, business development space began to embrace it. 15:00 All of those factors sort of pulled me in. It wasn't one thing or something that I actually specifically went out looking to, it was just where the world wanted to move and it's exciting, I like technology and that's how I got here. And having fun with it.

Healthcare to home security, how was that bridge made?

It's interesting, I think it was driven by two things. First off, I wanted to come and have an opportunity to move to technology and to have an opportunity to create something so that draw me into ADT and then ADT, which is not well-known by a lot of folks is that ADT also has a health business unit. So we're in the residential space, business space, and we have a health unit which is a natural extension of the hub that we have in the home.

I did not know that. I was going to ask about B2B but I had no idea of the health component. What is the health component for ADT?

Our health unit started and historically, it grew out of a very traditional personal monitoring device like a purse device. For listeners, a common thing there would be a PERS (Personal Emergency Responders) and as the technologies have developed; those devices are now like on technology steroids. For example, these devices know when someone has fallen.

You don't have to press a button.

Exactly. There's an accelerometer into it. There are exciting things about using geo-location data to help locate somebody. That particular aspect has really been a benefit of technology advances but also with the hubs in the home as technology evolves, it gives the ability to use devices so that consumers can be more educated, more in control of their own numbers, there are opportunities for them to work more closely with their doctors and their hospital systems. And for hospital systems and doctors, they work more closely with patients in a real-time setting. And that's helpful because it can drive quality of care and it can also help with things like when you come home from the hospital, maybe help address things like re-admission rate. It's all developing but that's the opportunity and that's what drew me is that there are lots of noble causes actually in the Internet of Things and in advancing some of these things and for me it seemed like a technology extension of what I had been doing in healthcare.

And obviously a lot of privacy issues there, too.

Why don't we jump in though? Let's get into privacy in IoT, what's your advice? What are some of the most important things that a manager need to know about privacy in the context of IoT?

This is an important question because I think no matter what the function is that someone is fulfilling in a corporation or company today, these things are crossing all sorts of lines and in fact, purposely crossing them and creating multi-stakeholder reviews and teams are really helpful to the notion of what we call privacy by design and that is very similar to the discussion that's been taking place about security by design where you actually start with some of these things in mind. For example, start with understanding what data the devices are going to be collecting. And in complementary to the security issues you would want to know that so you know how to secure them but in the privacy side, know that so you're thinking about things like, "Why are we collecting them? For what purpose? How are we going to be communicating that to the customer and explaining to them very transparently to serve the overall service that you want us to provide for you, it needs this information so this is what we're going to be collecting and how we are going to treat it, under what terms are we going to keep it, how you might amend it." And then think about your own manager, using a managerial mind then that leads up to in many of those buckets, 20:00 how do we do that in the best way? For example, one of the things I mentioned was communicating to the customers. So if you are a marketing manager and you're providing some type of services, you would have a lot to contribute to the privacy team about how we go out and talk to the customer, "in terms of our material, this is what we're doing" and then also helping innovate in terms of how simply you communicate that to people so they understand it, and how you go about getting those consents? There's literally a role for many different functional groups. In the makeup of privacy committees in the world today I think reflects that as not only a reality in terms of need but also recognition in behalf of companies in terms of who we're putting on teams and how we're thinking about these issues so that we try to do the best job because ultimately it's the trust. The customer trust then ultimately helps lead to the product being used so you can deliver the value that is behind the all effort anyway.

I think you bring up a good point, this cross-functional point because if you think about it even just a little bit, pretty much in every operational group there is going to be a privacy component, maybe in development it's more on the security side. To paraphrase you then, think about privacy in your role, perhaps join a privacy committee, perhaps contribute to privacy policy, am I getting you? What am I missing?

That's absolutely right, and reflect your function's inputs and needs. I think the cross-functional sharing of the process actually is very valuable to the organization and it's also valuable to what's ultimately delivered to the customer.

So maybe even galvanizing this type of discussion if it's not happening already? Obviously, there's a whole spectrum of companies that are serving the IoT market from startups to very large corporations. Maybe in startups they don't have this structure in place, even in the startup environment talking about this and I like your concept of privacy by design in parallel with security by design just to get this top of

mind, right? It seems like it has to be something just thought about from the very beginning.

I think that's true and just like security by design but there's a different nuance here and people may not understand it. When we're trying to encourage this across the development cycle, the functions and their influences change across the development cycle. For example, a marketing person's contributions over time change. Just to make my point, perhaps in the early stage their marketing is critical, they may actually be a greater voice in strategies later on but their input early on still matters. And why I'm saying that, you were trying to do this with the goal of having long-term customer trust, satisfaction and brand loyalty and various corporate functions and business functions play a different role at a different time across all those things. And so their emphasis point may be different but you want to have everybody involved from the beginning and foster this inclusion so that you get all these various considerations at every phase. They may be stronger for one function at a different phase but they're just as important for every function. And when you operate that way I think the environment is very rich and you can be picking up and delivering upon some pretty wide-ranging expectations overtime.

And I think just having different perspectives on that issue are going to, you're saying this which is unearth or uncover some points 25:00 that maybe others didn't consider. But I think it's really a cultural thing, I mean you've been in privacy and healthcare and then with ADT, do you think this is something and I know it's hard to get away from the security side of this, but is this something that's prevalent in technology companies? What do you think?

You mentioned that there might be smaller companies and they're getting started and there may be similar challenges to what we're talking about here to security by design issues that I've already been well raised in terms of the personnel that people have on board. With that being said, my personal experience and I don't mean to exclude startups because I've had the pleasure of talking with startups about these issues and at least you'll find somebody with a good understanding but I do think this concept of privacy by design is not new, it is being adapted well and there are other resources to help groups do it. You mentioned the importance of culture on top of just manning and other resources but i actually do think that there are a lot of reasons to be optimistic about this, there are a lot of people doing it right and making efforts to do it right and I think we ultimately see that in some of the rapid advances. If we just think of some of the rapid advances in Internet of Things apps from the privacy perspective, originally you would have, let's think a common thing about this challenge, about getting folks to actually read the privacy policies right and how that was a challenge or the bigger challenge was how long they were in the legal ease. So one of the things that I think is evolving is you've seen them using much simpler language now. Some of them are still long but they're making an effort to use simpler language. How about some of the really neat stuff that user experience developers have incorporated for special things,

for example, before you and I started the call today, the technology that we're using asked me do I want to turn on my microphone and my camera, right? That's kind of cool. And then we're also seeing people that are developing products take that to another level where you're beginning to see the incorporation of visual indicators if a Bluetooth connection is made, or at the top of your phone you can see indications that your location is being used, right? I'm not suggesting we're anywhere near done but these developments are coming with some fairly decent speed if you think about it. That to me is a good thing and it means people are innovating around them. As we already talked about, there's another mechanisms like IoT World and others to showcase these things and share them. I think companies are doing a really good job about that now. Gaps still to close, other things to still address but there are a lot of things to take pride in and to recognize people are actually not sleeping at the wheel here.

Let's clarify things because sometimes people conflate security with privacy, how would you contrast the two? Just make it clear.

They're very closely related so certainly it's understandable where folks think if I have security by design I have privacy by design. To keep it simple, both of these two sides will take credit for some of this, on the privacy side we're thinking about what data is and who should use it. on the security side we're thinking about what the data is and once it's decide that someone can use it, how do we get it to them? Once we decided what the data set we'd like to collect because it can help our product better deliver the services that consumer wants, how do we get that data to us securely is a security by design. Then once we have it, under what conditions are we using it, is privacy. 30:00 How we are talking and keeping the consumer abreast about that – that for me involves more of me. Though I work closely with security folks and try to have an understanding of it so I can be one of these contributors that I talk about, these multi-function contributors, the onus is on me to behave that way too so I try to stay smart about that so I can talk to it and understand when people bring things up. It's not my space, I wouldn't be the guy who wants to guarantee things are locked out or moving correctly but the privacy side, I am involved very much so in the robust discussion about what is it we want to use, how do we want to tell folks we're doing it and under what conditions?

That makes sense. Security being more of a technical issue and then privacy, you're defining policies so it's more of a business issue.

Yes. If you had those two circles, there's a center overlap where the two groups are working together and it's part of a strong link, you said that the outset in there do see me, you convey that I'm part of a team and that's sort of like those Olympic rings in the strong chain if you will. There are a number of functions involved but that would be how I distinguish between the privacy and the security side of it in the way that I think could be readily understood.

What about privacy and the bigger issue of liability? Because privacy is really an indicator of potential risk and a liability but it's not the only one, right? Within ADT, are you looking at privacy within a risk structure or is it separate completely from a liability or legal kind of liability structure? Am I clear on this? Do you see privacy as being a subset of risk so it's more underneath the legal umbrella because obviously you want to minimize the risk or is it something that's completely separate?

It's evaluated both ways. In terms of a risk evaluation, it's like any type of business decision you have to make is what is it you're trying to achieve, what are the inputs you're going to need to achieve it, and then what does that introduce, what considerations are being introduced?

For example, if we're talking about PII in privacy, if we have a customer that desires us to provide a service and bringing on that service to meet their needs requires a certain piece of information from them, then we need to evaluate well, is the benefit of providing it worth the risk of bringing that information in? and then you couple that next to your framework for securing that information but you do need to evaluate it because as we're all well aware, I think the big risk that everybody would certainly understand is that the right types of information other people might want to access who aren't authorized to access it and it needs to be protected and the more that we're involved in the Internet of Things and the way that these devices and services are being incorporated in people's lives and sharing information, collecting information that may not have been historically done or culturally done – these are risks and one needs to think about it. One of the reasons companies collect data is to improve products over time to improve their services over time, as all these devices begin to participate in these systems and more data is collected, there become risks that you have to evaluate in terms of when there's a security risk and then there are use risks – all of that can then lead to various legal questions that you'll need to work through. All of that adds up to what requires a very careful evaluation of it. But ultimately, I think it is a traditional analysis you're doing is that you're trying to say, "Can we provide what folks want to buy and what they need to live their lives better?" The requirements that we have to participate in that space, are they appropriate? Because you want to deliver a valuable product, you want the consumer to use it, 35:00 you want to meet their needs and you're pursuing doing it better than anybody else in a competitive setting. You have to do a risk evaluation for it but I think that's the trail all the time. No data is bad, it's just what data do you need to use and how are you going to use it and what's the good that's coming out of it?

Let's look at it from another way. What are high level and regulatory issues surrounding privacy in IoT because you want to use it in the right way, you also want to use in a legal way, what should our listeners be thinking about legally, regulatorally if that's a word, with respect to IoT and privacy?

From a big picture point of view, a lot of it could be traditionally discussed. We mentioned things like you need to certainly think about what type of data you're collecting, how are you communicating and getting consent to have that data, right? That's an important consideration. And then what processes do you have in place to keep that data fresh if you will, and accurate? This is heavily security related, but what processes do you have in place to secure that data in accordance with the way you've communicated that you're doing so just like your usage. All of that, I think can be traditionally bought over from other regulatory discussions applies but it just applies so with the individual nuances around Internet of Things and some of those nuances now is that they have this new special types of data. We mentioned PERS devices and geo-location tracking so there's other data that may have certain sensitivities to it. People's personal health information, which has different regulatory, depending on how you're participating in that space can introduce different regulatory requirements for people. The Internet of Things allows you to, and this isn't new or specific to the IoT but it's a global world and information is moving places and there are issues like regulatory issues now about where you store data and cross border use of data. These are things that existed but they certainly are having attention paid to them because of the Internet of Things and the types of data that are being collected. Then I think also particularly in security in home automation space, there are differences now being defined because of being in the home, right? And some of the ways some of these technologies require information or introduce the opportunity to use different data streams to bring value to people such as like video, audio collection. And now there's this you're not in the public space where you may not have an expectation of privacy but you're in your home, in a place that you cherish and keep private and that adds considerations.

Obviously there is a concept of do the right thing, treat the data as if it's your own. But there's also the issue of what's the legal framework, what's the regulatory framework? I guess what I'm wondering and asking you is for our listeners, to make sure they're on solid ground with respect to privacy, yes, do the right thing and I think your gut will help you there but do they need to go their lawyer? Are there other resources? But how do they know their own sure footing with respect to the law and regulations that are out there?

I would say absolutely. The earlier discussion we were having about the multi-stakeholder teams involved in privacy by design that includes if available to you your internal legal counsel, which could be residing in your privacy office, it could be in your business units, it could be both as well as outside counsel resources. There is absolutely a need to be working just like you would do any business transaction with good legal representation and counsel both generally and then also from specifically, if you're headed into a new area and you're using one of these sensitive data types 40:00 in the specific expertise maybe very appropriate. How would you know? I think there are some really good sources of information that one can touch on for free and at the fingertips. To get started, since we

mentioned security by design and some of the regulators, there's some really good information that's out of for example, available at the FTC about starting the security and there's some fundamental privacy things that are related in that story as well as the FTC as a nice report as does the White House has some information about big data and privacy and both these can be accessed.

I'll get these resources from you and put them in the show notes so people can click to them and review them.

Yeah, for example, the FTC back a number of years ago put out a book entitled something like "The Era of Rapid Change and Big Data". I'll get that for you. And then we mentioned the Internet Society; they have done some really great work in terms of Whitepaper on the Internet of Things, gives an overview, that's a nice piece because it talks about the security issues and then privacy, it does have a section on liability and legal consideration; it's a really good piece. Again, that was part of my comment why I think you'll find a lot of organizations and associations really getting this right and paying attention to it. And then even at your own informal programs. There's a lot of good resources there through other companies. I made some great connections at IoT World that led me to more resources and had me thinking about trust models, etc. I think just being involved in various professional organizations helps people get a lot of advice for free. You may have to dig deeper after you get it but I think it points you on the right direction.

I think that's important. I think everyone needs to just get on a certain foundation so that when they do go to seek legal counsel whether that's internal or external, for smaller companies obviously it'll be external, then they kind of know what they're talking about and they can utilize those resources at a more cost-effective way.

Yeah, they understand the issues and they've at least begun to think about some of the challenges.

I think that's good advice where there are some resources we could provide and then also like you were saying the industry organizations and associations will be a good place to start as well.

Let switch gears a little bit. I like to get your take, we've been talking pretty general but what's your take on B2B privacy versus B2C? ADT, obviously a big part of it I didn't know the healthcare side of it but B2C, but are there big differences there?

I think some of the questions that get asked are the same but on the B2B side you generally have good contract laws and considerations going into place to protect people. The evolving space at least from my perspective and I think where a lot of the attention we've been talking about for the last number of minutes in terms of regulators and policy makers does come in on the B2C side. I think some of that is because not only related to challenges about a collection and use and storage, which is important on the B2B side, every vendor

agreement, etc. and contract I've ever read is going into great detail on that and imposing contractual obligations on people. But on the B2C side, when you're working with the everyday consumer, this is where I place my attention and our focus in my office because folks don't always understand these things so we need to work on helping convey.

And then they'll have their own personal lawyer looking at it.

Exactly, and businesses have well established redress mechanisms. And so the consumer, where do they rely? They rely on companies first and foremost that they're doing business with and they vote with their pocketbook if you will and that's important because companies want to deliver a valuable product. Certainly in our case, we'd like to do that long term and it's helpful to the use of all our services that people engage in them and get the most value out of them. We have those pressures but then we also spent a little bit of time talking about the interest of policy makers and 45:00 regulators. For example the FTC, that's a consumer focus. We made the recommendation that people could even engage with their policy maker through constituent affairs. These are consumer issues and there's consumer protection laws and there's consumer protection mechanisms that are having this impact which cause folks like me to put our attention in the B2C area.

And on the B2B area, is it more or less covered already with existing mechanisms?

Yes, from my perspective, right? I better leave that up to some of my colleagues in the law department if they think there are some deficiencies but from my perspective and where my attention goes it's on the B2C side.

Within the B2C side, specifically for smart homes, connected homes, home automation, is there anything unique there with respect to privacy?

As I sort of said and in our particular space inside the home, it is unique and this is the traditional place where people has a really high expectation of privacy and they desire control and in the services that we were offering is because someone is trying to enhance their life but primarily they come to us because they're trying to secure their life and it's this blending of, in our space where we may have traditionally been trying to protect somebody's physical assets, now consumers are creating these digital assets, if you will and developing and evolving their understanding about them and so B2C and getting this right occupies my time and gets my attention because we want to do this right so that we fulfil those obligations and expectations. Just like someone would stay with us and companies like us to secure things over time, we want to be partners with the consumer and as I said, technology drew me into this field, the technology's exciting and looking forward to sort of delivering on that promise.

I think you brought up a good point earlier is when you're outside, maybe your expectations aren't as high but when you're at home, you're in own domicile, you expect things to be private. And it's interesting because I finally bought an Amazon

Echo, it's being delivered today actually. And here I am, I'm going to put this device right in the middle most probably in our kitchen area but it listens, right? They had to probably think about this a lot. I hear horror stories or I don't know if they're horror stories but about how the data is being collected and analyzed, every single thing that's being said in the home is being collected and then analyzed and then not acted upon obviously unless it's certain keywords but this is pretty big. I think it's even more in the home, just like you said, you have to be more careful because there is that expectation of privacy within your own four walls.

And these are exciting technologies, right? You mention this particular experience you're going to have today, I'm sure you're excited about it, right? And it's going to deliver value to you and your family but then again you want to understand what's going on.

Another resource that folks could tap into particularly that I think is helpful in this issue you're mentioning is this organization out of D.C. called Future Privacy Form. They actually have a paper they've done about always on, listening devices, which helps people understand some of the differences and these technologies so we'd be sure to list that in the resources that you make available.

Absolutely, I'm personally interested in reading that. And I'm going to be reading their privacy policy. I'm assuming it's going to be nicely displayed on the outside of the box but maybe I'll give people an update on that a little bit later on.

Paul, why don't we close with this, I'm just looking for some advice for management teams that are deploying IoT let's say into the smart home. What are some high level advices that you would give them?

To summarize the points I've already made is to build your review teams, your product design review teams where you're starting right with the initial problem that you're trying to address having multi-functional reviews taking place and that you're involved in broad stakeholder groups 50:00 so that you get all the issues and think about all of those things. I think I would also advice people to get a certain fundamental understanding and just do some minimal research which is readily available, we mentioned taking a look at the Internet Society, looking at the resources federal agencies make available. I think just some simple Googling about what types of factors are people putting into play when they make purchasing decisions. For example, the one you just made, you can find some relatively easy to read materials about how these technologies are advancing. So it's being informed and then what I would say is I think it is important particularly once you start getting an idea what your particular areas of interest are in terms of questions about what it is you're trying to develop, then you get the specific advice related to that either from your internal counsel or external expert counsel and I think that's a good way to get started.

Excellent advice. So you're saying effectively become familiar with the topic, lots of really good free stuff out there, surround yourself in these discussions with different

people within the organizations so you're getting different points of view and then bring on some counsel after you've done that when you're informed and you know your company's different aspects or considerations and bring on someone and make sure you're on the right track. Does that sound right?

Exactly right. Do your deeper dives in the relevant areas and I think that's a great way to get started.

Paul, how can people find out more about you and ADT?

For those who are interested you can find us on our website at www.adt.com. We're on the Twitter space at @ADT. You can find me on LinkedIn at Paul Plofchan and on Twitter. Send me a note, I'd be happy to engage specifically with anybody who wants to dig a little deeper into something I've said and I've enjoyed meeting folks who are interested in IoT. And thank you, Bruce for the time.