**RedZone Podcast Episode #84: Prepare For GDPR: Start With Privacy By Design Principles! – with Ann Cavoukian**

Bill: Sure, that's not a problem at all. We'll be, we'll be done well in front of that.

Ann C.: Great.

Bill:

[00:00:30] No problem at all. I know you and I talked about a month or so ago about a couple topics related to this and so I'm excited. I haven't started recording or anything but is there anything in particular that you, from our conversation a month ago that you think it would be a good addition or anything that you're finding a topic coming up that I could ask about that allows you to go into something that you find very unique or a different way or perceiving this?

Ann C.: I can't remember if I mentioned the new international counsel I formed on global privacy and security by design?

Bill: You did, yes.

Ann C.: Yeah, I'd love to talk about that because we had our fundraiser gala for that, it was a big success, it was sold out and all the big companies were there, Microsoft, Google, Deloit, KPMJ. It went really well. Maybe talk about that a little bit.

[00:01:00]  
Bill:  
Perfect. Yeah, I had kind of the four major things that I had captured from our conversation was positive sum mentality.

Ann C.: Yes, mm-hmm (affirmative). Yeah, for sure.

Bill: International counsel.

Ann C.: Yep, there's the international counsel, yeah.

Bill: The privacy is not about secrecy and freedom innovation and prosperity so we had some-

Ann C.: Perfect.

Bill: Yeah, some of the practical action steps-

Ann C.: And the GDPR.

[00:01:30]  
Bill:  
Yes, and GDPR, exactly, and then what people can do that you're finding really practical action steps people can take.

Ann C.: Yes.

Bill: Yeah, so this is good, so if you're good, I can start recording.

Ann C.: Yeah, let's do it.

Bill: Well Ann, I want to welcome you to the show today.

Ann C.: Thank you very much.

Bill: I think one of the biggest pieces about, I've actually been tracking you for a couple years and your work and so-

Ann C.: Thank you, Bill.

[00:02:00]  
Bill:  
I think you've been in the forefront for many years and it's taken a awhile, in particular since a lot of my listeners in the United States, the United States is a little bit slow to the party here with privacy, and I'd love to get your thoughts on the journey that you've been on and just a little bit about your origin story. How did it all get started for you and bring us right up to where we are today.

[00:02:30]  
Ann C.:

[00:03:00]  
Previously, I was the privacy commissioner of Ontario, Canada and for a long time, three terms, almost 20 years. During that time, I developed something called privacy by design in the late 90s but it really took off after 9/11. Two reasons why I did that, first of all, I'm not a lawyer, I'm a psychologist so most regulators, most commissioners are what I call lawyers lawyers, they love drilling down into section 29 sub three part A and applying that to the fact situations in getting a resolution, which is very important but in this day and age of massive, ubiquitous computing power, social media abounding, connected devices and IOT, it was just no longer possible to rely on regulatory compliance after the fact. We needed something proactive.

[00:03:30]

[00:04:00] I wanted to prevent the privacy harms from arriving the data breeches so I wanted a model of prevention, which would apply proactively before and you could embed the much needed protections into the design of your technologies, into your policies, your procedures, bake it into the data architecture. This model of prevention much like a medical model of prevention is what I came up with in terms of privacy by design. There are seven foundational principles to privacy by design, which form the absolute base of the foundation of your operations. Your actual policy and program can look 100 different ways as long as it reflects these essentials.

[00:04:30] That's how I came to it as I said, a long, long time ago, but 2010, it was unanimously passed as international standard, privacy by design by the International Assembly of Data Protection Commissioners and Privacy Commissioners. Then it's just been taking off and when we get to talking to the GDPR, that's another exciting development. This is what brought me to it. See, privacy [inaudible 00:04:31] is the foundation of our freedom. If you value freedom, then you value privacy because you cannot have freedom without privacy.

Privacy also fuels innovation and creativity and I would say it breeds innovation because you've got to be really smart to do privacy and other interests like security, like data utility, data analytics, you name it, you have to have both.

[00:05:00]  
Bill:

[00:05:30]  
Yeah, I do love how you talk about freedom because you know, I am not and not many folks in the US are, well, that's not necessarily true, not many entrepreneurs are for a lot of government oversight of anything. What I am a big proponent of is privacy because I think that comes to the founding principles that the country's founded on and I think that the technology, because the internet is really not that old. The real internet started in '95, so it's like I'm not sure, I know most of the general population just really doesn't know what happens behind the scenes in regards to privacy.

I love the GDPR is coming online right now because I think it's a big wake up call for the US and I think it's going to coerce companies into actually taking privacy seriously.

[00:06:00]  
Ann C.:

[00:06:30]  
Yes, well, it's going to be such a game-changer. The general data protection regulation, the GDPR, is literally with everything on its head, so first of all, it's one over-arching law that will apply to all of the 28-member countries of the EU. They will have to replace their existing privacy laws with the GDPR and develop laws that are compliant with that. The other thing is, for the first time ever, the GDPR actually has privacy by design in it and privacy is the default, which is the second foundational principle of privacy by design.

[00:07:00] For me, that is so exciting, but for everyone, it's exciting because it's going to be the exact opposite of what's happening now. Right now, you give your information to a company to use for a particular purpose but if you want them not to use it for any other purposes, you have to wade through the terms of service and all the legalies and the privacy policy to find the opt-out box that says, "Do not use my information for any purpose other than the primary purpose of the data collection, which is why I gave you that information," but we know nobody has the time to go through the terms of service and the privacy policy. Nobody does that, but it doesn't mean they don't want privacy.

[00:07:30] Concern for privacy is at the highest I've ever seen in the over 20 years that I've been doing this. It's at 92% of the population very concerned about privacy and concern for the loss of control over their personal data. This is huge. The game-changer is going to be once the GDPR comes into effect in May, privacy as the default says you, the company or the business or the government department, you cannot use my information for any purpose other than the primary purpose of the data collection.

[00:08:00] That's all you're allowed to do, and if you want to use it for some secondary use down the road, you have to come back to the data subject and obtain their positive consent. That is the biggest game-changer. It goes from black to white and that's why companies are just reeling over this.

Bill:

[00:08:30] Yeah, one of the things that what's really been interesting is that I was sitting down with a gentleman the other day and we were looking through his NIST review. It was a smaller, well, not small, but a 350-person insurance company so not an insignificant company. They had to abide by some pretty stringent standards and he's looking at this report and it's basically useless for him because it gives him no place to start, it just basically checks off a bunch of boxes. What he's got wrong and right and it's a cursory kind of overview and it doesn't actually tell him how to fix or how to do it, or how to do it cost-effectively.

[00:09:00] My biggest concern with all of these regulations imposed is how do you actually take action? How do you take positive action on it and because there's a lot of companies out there, and there's a lot of complexity with security?

Ann C.:

[00:09:30] Of course, and I don't want to be unsympathetic to these companies but here's why the regulators in the EU are going to be unsympathetic, because they've said, "Look, you've had five years to prepare for this." They take their time in introducing the legislation in the EU, literally five years. I think over five years, so this was introduced initially in 2012. The reason they take so much time is because they really want to be fair and give people a chance to ramp up. They don't want to just spring it on them.

[00:10:00] With due respect, five years is a long time and they shouldn't just be waking up to this now. Having said that, most companies are just waking up to it now and freaking out over like, "What are we going to do about this?" There are a lot of organizations, Trust Arc and others, who are offering primers on what to do. Anonymity is offering it too, lots of companies in terms of trying to make it simple. The ICO, the Information Commissioners Office in the UK has a document you can get from their website, a 10-step, "Here, do these 10 things. This is where you should start with trying to become compliant with the GDPR."

[00:10:30]

[00:11:00] There are tools out there available to companies as well as companies who are offering services on training others. I think you can get the help you need. One place to obviously start is privacy by design. You can get that on my website. As I said, I developed this years ago but it really took off actually after 9/11 because the essence of privacy by design is you have to be proactive, embed the much needed protections up front into your operations and also, get rid of the zero sum mindset of either/or. You can have privacy versus security, privacy versus data analytics. That's nonsense. That either/or proposition of one or the other, it's a win/lose model and it is so yesterday. Get rid of that and substitute positive sum models. Positive sum means you can have two doubly enabling programs in place that compliment each other and they can both gain at the same time.

[00:11:30] That's why I always say, have privacy and security embedded into your operations. You have to have both. Even though the term privacy subsumes a much broader set of protections than security alone, in this day and age of massive daily cyber security attacks, if you don't have security, you're not going to have any privacy. These are some of the basics. Get rid of zero sum models and get proactive. Get ahead of the harm. Try to prevent it from happening.

Bill:  
[00:12:00] Getting rid of a zero sum model means basically trying to choose between one or the other, security or privacy and basically what you're saying is embed both so you don't have to play either/or. Is that what you're referring to?

Ann C.: Exactly.

Bill: Okay.

Ann C.: Exactly. It's the either/or, win/lose model that's what's going to tank our operations. You have to have both and you can and must have both, let's do it. That's one of the driving forces of this.

Bill:  
[00:12:30] I know everyone at CIO Enterprise Innovation Series meets every six to eight weeks and I break it into offense and defense innovation and I believe that we're going to need to innovate in defense. I think defense is going to become the new offense. I think that companies that have a really strong defense meaning they can let their customers know that they're actually being good stewards of the data. Actually, that could become the new offense.

Ann C.:  
[00:13:00]

[00:13:30] I couldn't agree more. If you have a solid defense in place, so you have measures in place that will defend your operations from the onslaught of cyber security attacks and misappropriations of personal data for unauthorized uses by unknown third parties, if you have that in place, then you don't have to worry so much about the offensive because you'll be in a really good position to move forward from there. So much of this is getting ahead of the game, getting ahead of the harm and if you do that, I always tell companies, don't keep it to yourself, shout it from the rooftops. Tell your customers the lengths you're going to, to protect their privacy. That will increase trust, which is at an all-time low right now. It will increase trust and loyalty dramatically on the part of your customers.

Bill:

[00:14:00] Now, from your principles, your privacy by design principles, there's a clear way to drive costs down. Like we're often approached by companies that are about to launch, they call us when they have a beta of their app that's being released and all of a sudden, we look into the back end of that app and find that all sorts of people and personal data and everything's being put into that app. Now good thing that there is they're at beta, so they're not fully released but it's certainly more cost-effective to bake privacy and security into at the beginning of this process. What companies do-

[00:14:30]  
Ann C.:  
Hold on, but you're absolutely right. I'll never forget years ago when I was commissioner, it was Man Smart Meters were mandated in my jurisdiction by law, so every house had to have a Smart Meter attached to it and a lot of people were concerned about that because wirelessly, this information is being communicated when you get up, when you go to sleep, the amount of TV you watch can be inferred. This can be very privacy invasive.

[00:15:00] I went to my premier and they said, "Look, you've passed a law, there's nothing I can do about it." "Do you authorize me to build the strongest privacy protections into this," and he said, "Absolutely, be my guest." We did. We worked with all the energy companies and the power companies to develop the strongest technologies around Smart Meters in terms of wirelessly, encrypting the wireless communications that are to be sent out, et cetera.

[00:15:30]

[00:16:00] I remember a short while after that, and we published six, seven papers on this and we were contacted by San Diego Gas and Electric who at the time, in California, it wasn't mandated by law that Smart Meters should be attached to all houses, but a lot of the companies wanted to do this. Gas and electric companies wanted to do this for efficiency and better service, but they were getting a lot of push back. I remember they gave me this one story that their trucks were going into one neighborhood to install the Smart Meters and they were blocked from entering the neighborhood because the residents of that community drove their cars up to the front to prevent, to block the entry of these trucks.

[00:16:30] There was a lot of concern about privacy and other issues so they came down and they approached me and they said, "Would you come and talk to our board or CEO, et cetera." I said, "Of course," so I made my pitch on what we'd done here in Ontario and at the end, I remember one of the senior executives saying to me, "Well, young lady, you've made a good case, now what's it going to cost me?" I said to him, "With due respect, you're asking the wrong question. You should be asking, what's it going to save me? Because I can assure you, while there's a small cost involved obviously of doing this up front, it'll be the fraction of the cost you will incur when you start getting data breeches and privacy infractions, which I assure you, you will be getting."

[00:17:00] When there's a data breech now, it's not just a lawsuit that's launched, it's a class-action lawsuit, but the loss to your brand and your reputation may be irreparable. They signed on and they didn't have any problems. I also said, "If you do this, meet with your customers. Explain to them the lengths you're going to, to protect their privacy and how you will restrict your use of the information for the intended purpose, et cetera. Shout it from the roof tops that you're doing this."

Bill:  
[00:17:30] What are you finding out of your seven principles, your by design principles, what are the finding the one that's most resonating with everybody? Which one or two you find is most resonant?

Ann C.:

[00:18:00] I won't say it's the most resonant but the second principle, privacy is the default, is the biggest game-changer because it's the exact opposite of what people are doing now. Right now, privacy is not offered automatically without the customer asking for it. Privacy is the default. It builds it in right from the beginning. I think maybe the sixth and seventh principles would resonate most. The sixth principle is transparency. You tell customers, governments the information you have in your possession, that you've collected from your customers or citizens. You may have custody and control of that information, but it doesn't belong to you. It belongs to the data subject, the individuals from whom you collected the information.

[00:18:30] Give them a rite of access to your information and make sure they can see what you have. That transparency is not only good for them, it's good for you because you will never know if your information is 100% accurate or not. The data subject will bring to your attention mistakes that he or she notices. We found this again and again, it's a big help to companies to have data subjects actually access their data because it enhances the accuracy and the quality of the data.

[00:19:00] Even though that resonates with individuals because it's their data, they can access it, it also resonates with companies because it increases the quality, the accuracy of their information and it becomes a real win- win.

Bill: I wonder if ultimately there's going to be a data broker, like a master data broker or a couple data brokers that are going to essentially be like a wallet for your identity and for your privacy, that you're going to be able to hand that wallet out to Amazon for certain things, to your home mortgage for certain things, to a company that you want to be marketed and receive information for certain things, for your employer. Do you ever see that happening in the future?

[00:19:30]  
Ann C.:  
The only problem with that is then, you have to trust that data broker. I'll just point you to what happened with Equifax a couple of months ago, a couple weeks ago, I can't remember. They had a massive data breech and they just in fact revealed that it's much larger than they had originally reported. They were just weak on their security. They didn't go any upgrades that they should have done immediately. I'm very nervous with entrusting my information to groups like that.

[00:20:00] What I would much rather have something in works, it's called Smart Data, and this is the technology that will hopefully develop in the near future. Basically, the data itself will be entrusted with the permissible uses of that data. That data could be floating around in the ethers, in the Cloud or wherever, a company can only access it for the uses permitted, that is encoded into the data itself. Then if the company wants to use it for some unauthorized purpose, the data will effectively self-destruct for that unauthorized purpose.

[00:20:30] These are just examples. We're going to see lots of this kind of stuff with artificial intelligence and neuron networks. We want to embed privacy up front into these emerging technologies because I think that's what will have the greatest bang for our buck.

Bill: I actually think that Block Chain will be a huge win because essentially, someone's going to build an app that'll sit on top of Block Chain and it's probably no secret that this technology Block Chain's coming online in a practical way right about the time we need this.

[00:21:00]  
Ann C.:  
Yes, and there are companies like Enigma that came out of MIT. I think they're based in California now, that actually promise 100% privacy with Block Chain, which is fabulous because Block Chain is primarily a sudonamous venture but some information may at times be accessed if there are problems but they're taking that to even further levels like Enigma. I think it's very promising.

[00:21:30]  
Bill:  
I think I stopped you, you talked about transparency on your sixth principle in rite of access. Did you say seventh was important as well?

Ann C.: The seventh, yes. The seventh principle is keep it user-centric. Focus on the user. If you start with the user as the central hub of what you're doing, everything flows from that. Keeping it user-centric is absolutely essential.

Bill: Which is basically back to the foundations and freedom in the whole democracy to begin with.

[00:22:00]  
Ann C.:  
Yes. I couldn't agree more. Let me tell you, it's not an accident that Germany is the leading privacy and data protection country in the world. It's no accident. They had to endure the complete loss of all of their privacy and all of their freedom during the third Reich and when that ended, they literally said never again. Never again will we allow such outrageous outright surveillance and access to our personal information and our lack of total loss of freedom.

[00:22:30] I've been to many conferences in Germany, every conference is started with a reference to that time and they mean it. They're head and shoulders about other countries. They have not forgotten nor will they.

Bill: One of the questions I thought we'd talk about is the International Council on Global Privacy and Security. Maybe you can just let the audience know about that and sort of your role in it.

Ann C.:  
[00:23:00]

[00:23:30] Sure. Whenever there's an increase in terrorist incidents dating back to Charlie Ebdoe, Manchester, San Bernardino, London, Paris, the pendulum swings right back to, forget about privacy, we need public safety security. Of course, we do, but not to the exclusion of privacy and our freedom. Last year, one of my colleagues called me and said something like, "Get off your desk and organize some kind of international council. You've got a lot of international contacts from the time you were commissioner. We need to get attention to this, that you can have both privacy and security at the same time. We've got to rid the world of the zero sum either/or model."

[00:24:00] I said, "Okay." I tried to be agreeable and I formed this international council on I'm calling global privacy and security by design just to highlight that. We have the most amazing-sounding members. Michael Chertoff, he's the second secretary of homeland security in the US. Darren Entwistle is the CEO of Telus, one of our major telecos here in Canada. Gilles de Kerchove, he is the director of counter terrorism in the EU. I've got both privacy and security types. Greg Wolfond, he's the CEO of Secure Key, an amazing company that delivers privacy and security in a double-blind manner.

[00:24:30] All of these amazing founding members are forming my board. I wanted to get them to demonstrate that you can have both privacy and security types who both believe you have to have both of them, not one to the exclusion of the other. We just had our first fundraiser gala where all the funds raised here purely to go to research in emerging technologies and how you build this in. It was a huge success. It was sold out. Everybody was there, Microsoft, Google, Deloit, KPMG, PWC, you name it. All the big companies were there.

[00:25:00] I think it just resonated with the success of the idea that you can have and must have privacy and security. If I can refer anyone who's listening to this, if you'd like to go to the website, it's just GPS, S as in Sam, GPSbyDesign, all one word, .org. If you take a look at it, I'd love you to join. There's no cost to joining, it'll just show an agreement with the philosophy of we must have both privacy and security or privacy and data analytics. You name it. We can do this in a positive sum manner.

Bill:  
[00:25:30] There's a theme developing. This is this positive sum. Your manner in which you're saying, listen, we're not going to do this one versus the other.

Ann C.: Right.

Bill: We're all in on this and so I'm going to put your website of course and then I'm going to put also that you referenced privacy by design and all the companies that we mentioned like Enigma, Anonymity, Trust Arch, I'm going to put them all.

Ann C.: Yeah, great.

Bill: Just so people can reference them.

Ann C.: I would love that, thank you.

[00:26:00]  
Bill:  
Now is there anything that's on your radar that you just, any message that you can see for the decision makers that are out there? One of the things you had mentioned, when I mentioned the NIST piece because a lot of the, well, let me just frame this. A lot of the decision makers for enterprise and business have to look at frameworks or they are looking at frameworks. We're buried with frameworks, with NIST, with GDPR, with PCI, with HPAA.

Ann C.: Right.

[00:26:30]  
Bill:  
The CFO has the advantage because they just have gap accounting principles and AICPA standards and so we have all these frameworks on the security side so where, and GDPR frameworks will be coming out pretty soon as well.

Ann C.: Right.

Bill: Where does one start? What's a good start for someone that is concerned about what you're referring to?

Ann C.:  
[00:27:00]

[00:27:30] Honestly, I would start with privacy by design, the seven foundational principles. They're really straight forward and since privacy by design is now part of the GDPR, that will also help you. The other thing I just wanted to mention, the theme of privacy is good for business. People are often surprised when I say that because they think, "Well, privacy stifles innovation and creativity." As I said, it does the exact opposite. It builds, breeds innovation and it builds trust. Trust is at an all-time low right now. 90% of the public is distrustful of both governments and private sector entities collecting information. They're very, very concerned.

[00:28:00] If you want to build trust, you want to build loyalty, use privacy to your advantage. Gain a competitive advantage by telling your customers the lengths you're going to, to build trust and to protect their privacy. That you have great respect for them. This will preserve the customers you have and it will attract new opportunities.

[00:28:30] It's so important and it's in the spirit of transparency as well that you're telling them what you're doing. I think it just goes such a long way to building what is lacking now, which is a trusted business relationship. We've got to build this up from the bottom up. I've never seen online research like Pugh Internet Research polls at a high of 90%. They're regularly in the 90 percentile now, ever since Edward Snowden's revelations. 90%, 92% of the population being very distrustful of anyone collecting their personal information, government or business.

[00:29:00] They're fearful because they feel they've lost all control and they don't know what to do about it. You can turn that around by talking to your customers, telling them the lengths you go to, to protect their privacy, respect their privacy and that you want to work with them. I found that when you do that, and then you want to use their information for a secondary use, if you have that trusted business relationship, customers are happy to allow you to use it for additional purposes. What they don't want is their information being shared with unknown third parties and they have no idea what the third party is going to with their information. That's where they want the walls to go up.

[00:29:30]  
Bill:  
Yeah, and it's super practical. I mean, I just had someone the other day and had several millions and millions of dollars being made in different sources and they have to make hard decisions, they're using email addresses being collected to farm out to other services and they're making $100,000-200,000 a year in these kind of ancillary of income sources and they're going to have to shut those down because they don't have the permission.

Ann C.: Yeah.

[00:30:00]  
Bill:  
This is real impractical. Well, Ann, this-

Ann C.: With the GDPR, we should add that if you are found to be breeching the GDPR, the penalties that can be levied are enormous. 4% of global revenues can be charged. Imagine 4% of Google or Facebook, I mean we're talking millions of dollars here.

Bill: 4% of global revenues.

Ann C.: Yes.

Bill: Holy mackerel.

[00:30:30]  
Ann C.:  
Holy mackerel, exactly. Let's get up to speed and raise privacy.

Bill:

[00:31:00] I just think that security has always gone slowly and I think this is also another interesting thing is that with innovation on offense, the offense is playing offense and it's trying to go quickly to market and one of the interesting pieces, which I'm really interested in seeing in the next five years is how defense can change so that actually we bake privacy and security in but it is more fluid and can actually morph and change, not the level or standard change but it's able to morph and change with changes to business without constantly breaking and cracking the foundational principle.

The FBI wants, I mean normal cases, if the FBI wants to go and get information, they need a warrant. Even if they want to go fast, they need a warrant but then they just need a warrant faster. It's not that they got a warrant.

[00:31:30]  
Ann C.:  
You can get warrants online now so I mean it's nonsense that this stuff takes forever to get, that's no longer the case.

Bill: Yeah, so I think that that's the challenge that's going to speed things up for business.

Ann C.: Agreed.

Bill: Ann, I am so happy you came on and it is such a privilege for someone like you to come on our show and share your wisdom and your hard work over the years. It's I believe, paying off in spades.

[00:32:00]  
Ann C.:  
You're very kind. Thank you so much. It was my pleasure to do this.

Bill: Great, and I'll make sure all your materials are online and is there any other things that you want to share with audience or do you feel like that you've kind of made your major, we've learned your major thesis?

Ann C.: I think you have but I always like to remind people at the end, that privacy is all about freedom. If you value your freedom, then you value your privacy. Fight for it.

Bill: Thank you, Ann. I appreciate you for your time today.

Ann C.: Many thanks. Bye-bye.

Bill: Bye-bye.