KPMG

Customer First

Podcast transcript

"If you look at traditional principles that have underpinned our privacy laws, like transparency, accountability, and consent, I don't think that's going to be enough, because there's too much onus on the individual to protect themselves."

Voiceover: Welcome to the Customer First Podcast, from KPMG's Global Customer Center of Excellence. We work alongside the network of KPMG firms to help clients deliver profitable growth, by putting their customers at the heart of their business.

The Customer First podcast brings you the latest thoughts and market examples from KPMG professionals and guests on how today's businesses are becoming more and more customer centric. Today, we are talking about about privacy and data.

Julio: Hello, my name's Julio Hernandez and I'm the Global Service Line Lead for Customer and Operations and I also have the privilege of leading our Customer Center of Excellence. And I'm super excited to be having this podcast with you today.

Today's topic is the great data debate. And what we're really trying to frame up here is the need for data, the need to protect that data and getting the balance right between the consumers that you want to serve with highly targeted and personalized interactions to create really relevant customer experiences. And to offer personalization requires insights and data to fuel that. In addition, the organization needs to be able to protect the data that it acquires from its customers. But how can we ensure that we're actually doing this in the right way? How can we ensure that we're getting the right consent from our customers? How can we make sure that we're balancing the privacy and the trust implications of these interactions that require data?

From emerging technologies, like the metaverse and interactive, conversational speech-processing to rapid developments in location-based services, businesses are undoubtedly able to learn more about their customers than ever before, but they should also be careful with those insights.

55% of our respondents in our 'Me, my life, my wallet' study said that protecting their data was really critical to them and an important element to building trust. In addition, 47% of those same customers said they do not want their data to be sold. And they have absolute concerns about cybersecurity and hacks. And this is only increased with the advent in the last two years of COVID, with 6 out of 10 consumers saying that they were worried about their data being stolen. So how can organizations balance the quest for insights, versus the protection of this data?

So today I've got two great speakers with me.

First, we've got Sylvia Klasovech Kingsmill, Global Head of Privacy and Partner at KPMG in Canada. And we have Paul Henninger, the Global Head of Lighthouse in the United Kingdom. Welcome to you both.

So Sylvia, maybe you just give a little bit of your background for the audience?

Sylvia: Absolutely. I head up the privacy practice here in Canada. I'm also the global cyber privacy leader on behalf of KPMG International. A lot of the work I do is in privacy risk management. I am an attorney by training. However, the work that I do is primarily in identifying risk-based and privacy engineering approaches to protect privacy.

I've been with a regulator for quite some time before going into privacy consulting. And I have lots of experience in dealing with privacy program design and enhancement, but I also do a lot of work with clients, irrespective of the sector. So sector neutral, I'm all over the place, in dealing with the multi-jurisdictional privacy breaches, some of which have been highly publicized in the media.

Julio: Thank you, Sylvia. And Paul, could you just introduce yourself too?

Paul: Yeah, absolutely. So I'm a partner at KPMG, based in the UK and I'm Global Head of Lighthouse, which is our AI, analytics and emerging technology Center of Excellence. I've worked in data and analytics for about 27 years now and so as a result of having gone from being a practitioner to building practices in that space have been both tackling issues around user data, the ethical use of that user data, protecting that user data from attack and all sorts of other issues involved in that trade-off between responsible use of the underlying data and effective analytic solutions, to help our clients.

Julio: So as the privacy landscape evolves, consumers are more and more aware that companies collect and are using this information for a multitude of purposes. So what must companies think about around the data and what they can and should do with it? I'll, first of all, tee that up for you, Sylvia, so that you can share a little bit of your perspective as it pertains to some of the regulatory constraints.

Sylvia: So when you say, what we "must" do with the data versus what we "should" do, I think when you look at it from a regulatory lens, what we **must** do with the data speaks to the baseline, which is set in legislation. But I think the privacy conversation today versus 10/15 years ago when I started doing this work is "what **should** we be doing with our customers data?".

And that's fundamentally different than the "must do", because one is grounded in legal restrictions and prohibitions to avoid a fine or a penalty, whereas the other is about "what's the responsible, ethical thing to do with your customer data?" And that conversation revolves around trust.

We call it a Trusted Imperative[1] here at KPMG, because that's the underpinning for emerging technology. There won't be any user uptake or adoption of any of the wonderful new technology out there if the end user doesn't believe in it, if there's no trust. So there's a huge difference between those two and in the regulatory landscape around the world globally, there is massive change. It was spawned by the 2018 European reform legislation called the General Data Protection Regulation or GDPR for short. And around the world, there are GDPR-like laws being enacted. And in some jurisdictions, like the one in Canada, my home base, we're rather slow on the uptake. So a lot of our clients are looking to best practices, regulatory guidance and more importantly regulatory expectations, because everyone knows that the law doesn't catch up quickly enough to evolving and emerging technologies. So the right thing to do, the ethical responsible thing to do with customer data is to put yourself in the shoes of a customer. Think customer first, think privacy first with respect to how you're going to use the data, how you're going to protect it.

And I think that's really important, with the Trusted Imperative that we have, that we preach to our clients. Because that's going to set a company apart from the rest, right? Forward-thinking organizations are going to have to understand the advantage of bringing together all the aspects of the privacy user-centric model of doing things, with respect to privacy notices, cookie management, consent, subject rights, and all of that good stuff.

Julio: So Sylvia, you laid out a tremendous amount of information there. Like GDPR, like trying to be customer-first, walk in the customer's shoes, but the power dynamic around this information, where does the end consumer really have the most control?

Sylvia: Well, that's the whole issue here. There is an imbalance, because everything is based on a willingness to share data, data begets more data. However, the historical battle between the end customer and the data collector was always the imbalance of power, right? The loss of control once you give up your data, because the customer has no idea where the data's going or how it's being shared.

And if you look at almost every aspect of our lives today in the digital world, it's being mediated by great social media platforms and it's influenced by their goals, which really is employing machine learning, trained algorithms and dozens of professionals whom I refer to as data miners, they observe, they map, they track, they catalog and they manipulate our online choices and our behavior.

And this is where privacy comes into play. It's about digital dignity. About the control of your own personal information, which is much more than just consent over how the information is collected, used and transmitted. Really it's about autonomy, being free in a digital world. And again, that's all predicated on trust.

And if you look at what legislators and regulators are doing today, they've begun to address non-consensual use of data, microtargeting, manipulative user interfaces, automated decision making. They've begun to develop innovative rules to rein in all the abusive design choices and to put substantive limits on data collection and subsequent use of that data, which is referred to as data minimization.

There is now duty of care. There are rules around conduct, ethics, restrictions on bias, there's rules around discrimination and the use of AI. And so really, I've even seen outright bans by regulators on particular technologies, like facial recognition. So if you look at traditional principles that have underpinned our privacy laws, like transparency, accountability, and consent, I don't think that's going to be enough, because there's too much onus on the individual to protect themselves.

People are so overwhelmed when they're online. With all this new digital technology and the choices out there, there's no practical alternative, but to click "I agree" or "allow tracking while using this app to get a seamless customer experience". And that's the imbalance that I'm talking about.

Julio: Let me pivot to Paul because you said a couple of things there, one might say might be provocative.

So you used terms like "manipulative" and "forced choices". But at the same time, Paul, data is the fuel to make some of these algorithms work, to be able to deliver a better customer experience.

In your view, how have you seen bringing the technology to this data in a way that, tends to demonstrate some more trust, some more principles, if you will, in the engagement with the end consumer?

Paul: I think first the thing to keep in mind about the way in which our data is being used to present choice to us is that one of the things that's come along with this digital transformation we've all been in the middle of for at least a decade, if not 20 years, is that the experience we have of interacting with the people we purchase things from, the people we do business with, the people we bank with is not infinitely configurable, but very, very configurable.

If I walk into a shop, the shop looks about like it looked a month ago with some slightly different things up front; the website that I interact with, whether it's social media or my online banking can be changed every five minutes if they want.

And so someone can and does often make the decision what to present to me. And that's where data comes in. What's the best thing, what's the most useful, most valuable thing to present to me? And I think it's that topic, that issue of value, which is the key to a responsible use of data that customers will understand.

A good corporation or organization these days will ask themselves two questions. One: do customers understand how we are using their data today? Second, and perhaps the most important: does that use of data present something that's clearly understandable as valuable to the customer?

[1] https://home.kpmg/xx/en/home/insights/2022/01/the-trusted-imperative.html

Paul: And if those two things can come together and if the distance between them, isn't that great, i.e. that the customer understands that "they're going to use some of my data to do something that I'm going to enjoy or find some gratification from", and that thing actually legitimately is valuable to the customer and they can draw the line between those two things and don't think it's an inappropriate line, then you get an excellent customer experience that's an improvement for the customer and one that they feel comfortable with. Which can have a knock-on effect of them getting more comfortable with the use of their data to begin with.

Julio: You used the word knock-on effect, and Sylvia talked about the unintended consequences. Part of this is a perspective over time, right? I might be willing today to give up more information that I might be willing to give up in five, or 10 years, but now that information's out there already.

And so I can't really put the genie back in the bottle. We've also seen recently certain companies have actually really started to constrict their privacy policies. In fact it's made certain other companies that had advertising businesses decline in value, because that privacy was being constrained.

So Sylvia, when you think about that, this idea of this, time-based view, how should companies be thinking about what they're doing today versus what they might be doing in three or four years with that data. And what kind of power does the consumer have to say, "enough, I don't want you using it anymore. It was great you using it for the last 36 months, but now I want to wipe the slate clean."

Are there any options to the consumer around that?

Sylvia: So first of all, I wanted to address your question around– and what Paul was talking about–the value exchange. And I think the empowerment of the customer to have the choice to make an informed decision about how much data they're willing to give up and what they get in return by the company that collects the information for a trusted, seamless experience.

And I think there's a paradigm shift happening. I think companies are beginning to understand that reputation is key, trust is key, and that they're in it for the long haul. I don't think customers are willing to jump around from one company to the next if they trust the companies that they're with.

And we need a lot of data to ensure a good customer experience, to understand the customer better, to drive intelligent insights and to do more with data. Now I'm seeing, a complexity with respect to AI regulation, for example, around data minimization, where we're trying to comply with data minimization principles, yet we need a lot of data to avoid bias. We need a lot of data to make informed choices with the data, in terms of targeting individual customers.

But I think that can be balanced and that can be done if we start giving back some of the control to the consumer through transparency and better notice.

And how do we do that? We inform the customer through real-time notices and short consent forms that are meaningful to the end customers so that if they make a decision today, they will understand and appreciate the consequences years down the road, so that the relationship is fostered over time. I know a lot of great companies who try to do the right thing, but they're overwhelmed with overregulation or not enough funding to put privacy specialists and privacy engineers into place to ensure that all the right safeguards are in place to protect the individual customer.

If you do the right thing, if you're transparent enough and there's a willingness to be open about consumer choices, I think that the customer will remain loyal and you can do a lot more with their data.

Julio: I think one of the things we wrote about a couple of years ago was this concept of permission and presumption, right? So I might give you permission to use my data, but I had a presumption about how you were going to use it. I presume you were going to use the data to give me better offers and to tailor what I would see.

That was one element. But when I started to get messaging that might have gone into the political realm or into other areas, it started to get a little bit more complex. And so it was this idea of permission versus the presumption. And I think, like both of you said, there's this need to establish trust with the entity. But nevertheless, it's hard because that presumption changes over time, as well as the permissions and different people are tackling it from different ways. Regulators are tackling one way. Certain companies put, like you said, their own privacy officers in place and all the rest, but yet there's this insatiable thirst for getting closer to the consumer, getting closer to customer, building out these insights. And a great example of that is large corporations moving into the metaverse.

Paul, I'm curious, what are you seeing out there in terms of companies maybe rethinking their data strategies where they may be able to have a much more direct relationship with the consumer in the metaverse?

Paul: I think for the most part, the companies that we're working with and talking to are extremely excited about the prospect that the metaverse creates. And I think there's two reasons for it. One is that it's definitely the case that quote, unquote "companies have more data on us than ever before", but that is not uniformly the case. The ones that get in the news that have gotten in trouble for user data abuse and things like that, the big media platforms and things, they have tremendous amounts of data about us, but some of the brands that we all know and love, big consumer brands don't have a direct connection with us. Their connection is mediated by distributors and retailers and other websites.

And I think one of the things that the metaverse presents is the ability to create an experience whereby they have direct interaction, where they can start to put their products, new digital products, new services, new experiences, and see what customers are interested in and create much more direct feedback that is almost by definition permissioned.

The reality is if you take large soft drink manufacturers' online experience, if it's fun and I want to be there and my friends are there, I will go back there. If I go there once and it's not that interesting, I'm not going to go back and they're not going to get much of my data.

Paul: I think people are very excited at the prospect of that. I also think speaking of your last question, in terms of the time span, that there are data privacy concerns, which you've only just started to tackle that we need to be aware of so that we don't back ourselves into another one of these morasses of, "we didn't realize we were doing all this with data".

And I think in particular around some of the applications of metaverse that are probably more like three or four or five years out, in particular, the use of AR and VR, the idea that I could put on a headset and be immersed after 5:00 PM in some kind of cool new futuristic universe is amazing. But the data that's collected by those headsets is literally every square inch of my room that I have it on in. So all of a sudden, the tech providers or whomever, somebody potentially has access, not only to my preference in terms of which stuff I click on, but, like, where I put my couch and how wide it is and how far away it is from my television and how many people are in my living room with me and all sorts of things like that.

I don't think that's been something everyone's concerned about, because we're way far away from that being a problem en-masse, but it's one of those things we need to keep in mind as we design these experiences that we continue to keep privacy at the forefront of the new things that we're testing out with consumers.

Julio: One of the things that Sylvia said at the beginning of the conversation was that this stuff tends to get ahead of itself, right? And the regulators and others have to catch up. And so businesses probably need to be thinking about this in multiple dimensions.

One is, what's the business opportunity for me able to harness that data? What's the appropriate way for me to harness that data? What is it the consumer wants from me so that I can provide a better experience? And what are the regulators going to do at some point to basically put guardrails around that? Sylvia, when I think about that, and I think about your background as a lawyer, as someone who's worked with the regulator, as someone who's advising clients around this space, if you were talking to a Chief Financial Officer, how would you explain the long-term benefits of investing in a strong privacy policy and the dollars and the energy that goes into that? And how would you justify that business case to make sure that the company spends time on that?

Sylvia: Great question. Privacy policies historically were laden with 'legalese' - inexplicable terms that no one could understand in street-friendly language. What is the data that we're actually collecting as a company? What uses are we going to put the data to? How are we going to protect it? What's the value exchange? I keep on going back to the value exchange, because I think the end customer is really interested in the value that they receive for giving up their data set. And I would say treat your privacy policy less as a legal document bound by law, make it into a marketing tool, right?

Make it short, make it simple, street-friendly, so that customers feel more empowered. They understand that they can trust you. And I think the substance of that document should really be about keeping the data safe and living up to the commitment, with respect to data use.

Often I see a disconnect between the information handling practices on the ground when I do privacy risk assessments and the policy statements around what the company is supposed to be living up to and how they're bound by privacy legal rules. And that's the stuff that gets companies into trouble. That's the stuff that creates the distrust between the customer and the data collector.

Regulations, as I noted earlier, don't keep up with the pace of technology. So it's about managing expectations, whether it's the end user, the end customer, the regulator, it's about getting ahead of the baseline requirements at law and taking a privacy engineering approach. I call it privacy by design and security by default, where we're advocating to companies to start hiring more privacy engineers to look at privacy less so from a policy point of view, but more from an engineering design point of view, where we're building the right protections into the architecture of the system, into the fabric and the culture of the organization.

So for example, with privacy engineering, it's really a trend where you're looking at the code and the personal information itself to identify privacy issues with the logic. It's an emerging discipline really out there, where you're looking at static code analysis, like the cybersecurity guys used to, and we can adapt and adopt it for privacy code analysis, so that it's more of a holistic approach to privacy, looking at people process, governance and primarily the technology itself.

Julio: So Paul, building on this idea of privacy engineering, and I love that term, do you have examples of how folks are safeguarding their data activities and leveraging technology, in addition to processes and rules, to be able to protect data?

Paul: I think there's a couple different ways we're seeing people start to do that in a good way. So the first way, and that comes out of some of the things that Sylvia talked about, for example, privacy by design, is building into the very early stages of a design – of a new experience for a customer that's driven by data, a new model that's trying to forecast actions by a customer and present them with options, or simply forecast sales or attrition or something like that.

One of the early steps in those model development processes is increasingly in good practice to take into consideration whether the types/amount/sources of data are those that are appropriate for the application, rather than coming in at the end, once this beautiful analytical object's been shaped, and trying to unpick it somehow and strip out the stuff that was ill-advised, or just having to force yourself into a decision about the trade-off between performance and privacy.

So involving privacy up front, alongside a lot of other things including user experience and outcome, and "how do we measure success?" and things that weren't always part of that initial, often very technical, design were quite critical.

The second thing is what we are seeing is the relative early stages, but moving very quickly, of a re-architecting how we store, transport and make use of data. Part of the reason this was so difficult and part of the reason it felt so frenetic and a little bit out of control when GDPR came in is that data was kept all over the place. You've got relational databases that have some data from 20 years ago in them. You've got these new databases that we put onto the website or to the mobile application that had a bunch of data in it. And companies and organizations have started to rationalize the different types of things they want to use with data. They want do data science to do research. They want to do operational analytics in order to create better experiences for customers, in order to get competitive advantage, in order to cut costs. The use of data lake technologies, data transport technologies, has forced people to go back and rethink the architecture that they have to collect, or to move and review the data that they have.

Paul: And as part of that, it's natural for good practice to build a periodic review of "how long have we had this data? Is it still permissioned? Is it still permissioned for the types of things we're using it?" into the literal storage of the data itself. And it's only recently I think that people have really started to have projects and initiatives that are consolidated enough and that have learned the lessons from the past, both technical, ethical, and functional, that we're in a position to start doing that well.

Julio: Sylvia, you talked a little bit about doing some privacy audits at some clients and going in there and seeing how things are working. And you said you see breakdowns from the intent to actually at the coalface level sometimes. What are the key pitfalls businesses should be aware of to avoid appearing to dismiss the customer concerns over the use of their data?

Sylvia: The biggest pitfall is the disconnect between people, process, governance and technology. That's really critical. I think privacy governance is largely overlooked in a lot of the organizations that we work with. Who owns privacy? Where does it live? How do we run a successful, optimal business through privacy-enhancing technologies? Because usually the business is complaining that "doing all this privacy stuff slows us down in the market. We're not agile enough to get out there." And then the Chief Privacy Officer or the Chief Auditor gets nervous around reining in the business, to ensure that there's compliance and to avoid any risk of penalties and privacy class action lawsuits.

Every large breach that I've been involved in in the first sort of business is "okay, does the organization actually have a tone from the top and make it part of a business strategy to protect privacy and where does privacy sit and who's looking after it?" Number two is over-collection of data and over-retention of data. The two go hand in hand.

Regulators are really fussy right now around the collection and use of particular identifiers and I would really try and focus on classification of data discovery, understanding where your data assets are and try to purge or dispose of data that's no longer in use. And if you have a retention policy for keeping data longer than the retention period or otherwise, then ensure you have a defensible position with the regulator around the business purpose or the data minimization techniques that you're deploying to protect the information, because the more data you have, the larger the risk with respect to the attack surface and all of the bad stuff that the data hackers can do with the data once they're in there.

Paul: Just to pick up on that. One of the things that I've always made sure my data science teams look at is the idea of too good to be true. We have seen a number of times that even when someone builds a model, it could be a complex machine learning-based model, it could be just some basic statistics and they find a data set that allows a massive amount of lift in the model. That's exactly where you need to look to make sure you're doing the right thing.

There was a case where we were involved in a bunch of people trying to figure out the deployment of a new lending model that predicted probability of default. And what we found is that the use of unconventional data sources, people's online behavior, all sorts of other information could produce lift that was many percentage points beyond what people had been able to do historically.

What we asked ourselves was: "are we sure this type of data is appropriate in this type of context?". When you get the massive performance increases that are too good to be true, you also have to pull up and ask, "are we sure that the distance between when this data was given to us, for a certain purpose and what we're using it for today and the amount of time that's passed is appropriate and defensible and obviously within regulatory restrictions?"

Julio: Both of you guys gave examples of financial services and so, as I think about this area, just like a financial advisor goes to their customers and says, "what are your objectives that you want to achieve with your investing profile?", what requirements are there today in terms of companies revisiting with their customers, what they want to get from the data?

So while I gave you permission a year ago, or five years ago, maybe I need to check in with you every so often to make sure that the objectives you want to have achieved through sharing data are still appropriate, given where you are in your life. Are you seeing any regulation around that?

Sylvia: So, what I'm seeing is that regulations are evolving. Regulatory expectations and customer expectations are also evolving. And I think there's a lot of new technology out there, like AI, that we're just trying to understand.

And so this is not a static exercise. You don't stand up a privacy program or you don't build a privacy enhancing technology and let it sit. I think you need to take a risk-based approach to everything you do. I would advocate to do impact assessments, for example, to set up a data governance structure that's meaningful and to have human oversight, not because these are legal requirements. Remember the conversation around what must be done with data versus what should we do with data? I think these things are important because that's the right thing to do for your client's data and to foster that trust.

Paul: As Sylvia has said, one of the things that people are getting much better at across the board is simplifying and clarifying, when this initial permission is given, that it's clear that someone has a chance of understanding it. I think that's the bare minimum and it's partly the way it is because it's increasingly enforced as a sort of behavior that governments and regulators say you have to do.

Good practice that we're started to see comes mostly I think out of collaboration between organizations. So you will see fin-techs, for example, who offer you the opportunity to attach their service to your online retail platform of choice or some other kind of major part of your digital life. And it's clear when you attach those two things, that there's data flowing back and forth between them with the value proposition that your banking experience is going to get better on the one side and that your retail experience is going to get better on the other side. And also the explicit promise that you can detach that at any point that you no longer feel it's something you're getting value out of. And again, if you read far enough into the data privacy agreements, that data will no longer be exchanged.

I think there's a lot further that we can go. I do think that we will start to see people get competitive advantage out of coming up with creative ways to ask clients: "how can we better serve you with the data that you potentially could give us? Not just the data that's coming back and forth in our interaction, but other interactions you have with other organizations that you do business with that that might help us serve you."

Julio: What do you think the correlation is between your privacy policies and your brand?

Paul: I think they're strongly correlated, but mainly because a lot of brands are valued similarly, and a lot of privacy policies have gotten quite similar. I think there's still a lot of opportunity for companies to distinguish themselves by a public, differentiated, aggressive approach to privacy. There should be a sector leader from my perspective: who's the retail leader in privacy? Who's the banking leader in privacy? Who's the insurance leader in privacy? And I think those positions are largely, across most sectors, quite open. And there's an interesting brand opportunity for people to start to claim that, see where that gets them.

Julio: So as we're closing out here, I'd love to ask each of you this question: what is your number one tip to a business who wants to improve their data strategy, while at the same time, putting in the right safeguards to protect their customer's privacy?

Sylvia: My number one tip would be start with culture. I think all of these transformational changes that need to happen with respect to leadership around privacy and privacy by design, privacy enhancing technologies, it's about finding commonality and shared values, beliefs, and norms that really foster trust-inducing behaviors, and that all needs to be aligned with an entity's purpose.

And so I don't think you can get very far if the leadership and the management teams don't have that tone from the top, who don't inspire or really believe in privacy. Because doing privacy for the sake of compliance is just the wrong approach altogether. If you believe in it, you have a culture, the values, the norms, and the beliefs, then I think you're going to get your business to move on that a lot faster than you would without that cultural underpinning.

Paul: I think a good starting point for anything is to measure things. If you can try and succeed in measuring the degree to which you are protecting and safeguarding your customer's data and turn that into something that you can measure over time and manage over time, then I think you've made tremendous progress.

I would say as well, there are arbitrage opportunities in this market. You can invest against the grain. You don't have to exclusively invest in technologies that assume that we're going to have everybody's data forever. And there's other places to look to find competitive advantage, using analytics, not just the sort of conventional brute force stuff that historically has led to a lot of success.

Julio: Well, Paul and Sylvia, I really appreciate you guys joining in in this dialogue around the great data debate. And clearly there is still much to be spoken about and much to be navigated as we move forward. But what you both did talk about was really harnessing this data in service of the customer and really trying to give them a better experience. The closer that companies stay towards that within the constraints of the regulators and with the right culture and with the right measurement systems, companies are going to have a much better and hopefully clearer path to moving forward.

Thank you for joining us. We appreciate you listening in today.

Please take the opportunity to visit our website around more customer insights and other episodes of our series. You can just search under KPMG Customer First.

So again, Sylvia and Paul, thank you for your time and to the audience, thank you for listening. Have a good day.

Listen to this episode and the rest of the series on Apple Podcasts, Spotify, Amazon, and Google Podcasts

For more information, search 'Customer First podcast' or click here.