Deloitte TECHTalks | Episode 18 | Building Digital Trust
*With Tanneasha Gordon, Principal, Deloitte & Touche LLP, Cybersecurity*

**Raquel Buscaino**: Welcome to Deloitte TECHTalks. I'm your host, Raquel Buscaino and I lead Deloitte's Novel and Exponential Technologies team where we sense, and make sense of emerging tech. On today's episode, I'm delighted to be joined by Tanneasha Gordon in Deloitte's Cyber practice, where we're going to be talking about trust, and even more specifically, trust in digital products. We'll chat about what makes a digital product trustworthy, what challenges companies and consumers face in developing and using trustworthy products, and what actions society can consider to improve safety and security.

Tanneasha, welcome to the podcast. It's really so great to have you here. And I'm just really looking forward to this episode.

**Tanneasha Gordon**: Me, too. Thanks for having me. I'm super excited for this discussion.

**Raquel Buscaino**: Well, you know, the focus of the episode is all about building digital trust but before we dive into the details, what do we mean at Deloitte when we say trust? And how do we even define digital trust in particular?

**Tanneasha Gordon**: So trust is a word that I know, that gets thrown around every day in terms of "Do you trust people? Do you trust institutions?"

And it could be kind of amorphous and hard to wrap your mind around. But at Deloitte, we see digital trust as the earned confidence and reliance in a company's digital product by consumers, patients, users, regulators and shareholders.

We focus on implementing and operating and scaling privacy, safety, security, and resilience solutions in service of that. And what do I mean by in service of that? It means we're looking at solutions that are reinforcing transparency and good data practices. We are looking to make sure that these digital products empower users and give them control over their data and digital experiences. We are working with product engineering teams to ensure that these products prevent and protect against online harms. And that these platforms aren't being misused by bad actors to proliferate abusive content, or even to just break the integrity of the technology stack itself.

We also are working with product teams to enable trusted and authorized access to digital resources, including data but also ensuring that there is fairness and ethical and compliant approaches as it relates to the data that some of these products are just collecting in an ambient and in a persistent way. So that's how we are thinking about digital trust and it's all about making sure that these digital products assets, services are putting forth the right safeguards to enable privacy, security, safety, and resilience.

**Raquel Buscaino**: Wow! You listed quite a few different things there. It sounds like trust is a pretty comprehensive definition, but I also like what you said about the earned confidence piece of this because trust is earned right there are things that you need to do to be able to enable it and provide that confidence to your users.

**Tanneasha Gordon**: Absolutely, and what we mean by digital products are anything that is technology driven, right? So a technology driven asset that is designed to deliver some sort of value through digital experiences.

So think of things like, software application solutions, social media platform, spatial computing platform and experiences, connected devices, anything where there is user interaction with some sort of digital experience or environment, where social networking or content sharing is part of that experience, where communications is facilitated, whether it's through people, communications with people or communications with AI, and experiences where the physical and the digital world sort of integrate. So think about those AR/VR related experiences.

Raquel Buscaino: Trust is a broad definition. Digital is a broad definition. I would love for us to be able to analyze a use case and break it down. And you mentioned interaction, social interaction in particular. So maybe social media would be a good example for us to dive into. What are some of the issues that are currently arising in the digital products that most people use?

Tanneasha Gordon: So, if we're talking about the areas from a cyber perspective that we're most concerned with at Deloitte, and we think are the best levers of building trust, that's privacy, security, and safety and resilience.

So the types of issues that we're seeing in social media as it pertains to those specific domains includes anything from like account takeover and hijacking, sophisticated phishing attempts through e-commerce interactions or fraudulent ads for example, which provide some of the security components that are very important and concerning. But then you have things like misinformation, disinformation, bullying and harassment, so that's where the safety component come into play, but when you're thinking about the data that may be harvested or the sophisticated attacks by bad actors, such as impersonation, right, we've seen a couple of celebrities get impersonated with the use of these really sophisticated deep fake tactics that can hurt someone's brand and also have mental health impact on an individual but also have a level of privacy infringement associated with that.

So these are some of the social media, what we would call “harmful behaviors” that we're seeing online that a lot of social media companies, digital platform companies have to contend with and ensure that their platform could be trusted by users, by parents, by governments which they're highly regulated, where you're seeing a lot of these regulations pop up in the U.S., like the Kids Online Safety Act or in the UK, the Online Safety Act, but these are the issues that some of these social media companies or digital platform companies are having to deal with. So those are some of the things that we're seeing.

Raquel Buscaino: I like the way you broke it down into the examples where security is maybe safety from bad actors, and safety could be bullying harassment, and privacy is how you think about data policies. And you know you mentioned that these three things are levers to be pulled. Do they ever conflict with one another?

Tanneasha Gordon: Yeah, that happens quite a bit which makes it a little bit difficult for some of these digital platform companies.

The challenge is when these platform companies want to intervene, or what they would call “intercessials”, is very hard to do that, because they're not supposed to be collecting information. And then, how do you intervene when you have to also protect privacy can social media platform companies alert a parent, for example, under GDPR is very difficult for them to do that.

Raquel Buscaino: That's a really good example of how safety and privacy kind of conflict, where both are levers of trust, both are designed in there to help protect end users. But in some cases they can conflict.

So we've been talking mostly about social media right now, which is just one component, as you mentioned of a digital product or digital experience. My team at NExT [Novel and Exponential Technology] talks all the time about the future of interaction technology, so AR/VR, extended reality, how GenAI might play a role. What are some of the examples of recent issues and concerns that are coming to light in this trust context, just simply because of the new technologies that exist?

Tanneasha Gordon: That's a really good one. If you look at a lot of AR and VR environments, it's required for that type of technology to collect a lot of data and to record individuals and their surroundings. So when thinking about digital reality systems like AR/VR, they collect way more personal information than any other traditional system that we've ever seen.

Its eye tracking technologies tracking your retina that combined with other biometric information that's collected can be seen as like a treasure trove of personal information. And from a scientific perspective, you can start to predict behavior based off of retina movement.

That makes that type of information that much more important for there to be safety and security controls and privacy controls around because imagine the misuse of that data being used to predict that you want a new house, a new car, right? We already think that they're listening but what they're doing is like, just your digital behavior can create like a psychological profile of what you might want to buy. So those are some of some of the challenges just from a privacy perspective.

I was looking at some new AR glasses that came out recently. And I love this technology because you get to have a first-person experience. Let's say you're on a roller coaster, or you are sightseeing in a really cool place you get that first-person recording. But let's say we're in the same place, how do you consent to me recording you?

Raquel Buscaino: I was just about to ask that because it sounds like, what's one issue when it's I as the user or aware of these devices, now have an extraordinary amount of data that's collected on me, right? Simply to make the device function. So the same levers are there but it's just the data explosion and the ease of access to that data.

But to your point that you just brought up, what does that mean if it's recording my external environment for those in my surroundings? And what if those people in my surroundings could be minors? And so it just brings up a whole other additional layer of data privacy almost at the collective level where and that could differ by regulatory and legislative processes, too, it seems like it's an ever increasingly complex web for different organizations to be able to operate in and thrive in, but also for consumers to navigate as well.

Tanneasha Gordon: Absolutely, and it's going to continue to happen, right?

Raquel Buscaino: So are there other examples of what organizations or what individuals could do to make sure that they're positioning their company or themselves for a more trustworthy future with digital products?

Tanneasha Gordon: Absolutely. We're always recommending to find ways to embed trust within your product development lifecycle.

And what does that look like? It really looks like finding ways in from the design. What are you designing and building? Like little basic product design features that should be embedded within the concept stage of that product design and development process.

Making sure that you have policies, design patterns and design specification as well as safeguards that are required for these digital products, available to engineers so as they're designing, they should cover privacy, they should cover security, they should cover safety, they should cover also resilience and transparency, which cut across all of those as like more of a horizontal to the 3 verticals: privacy, security, and safety.

And then before launch, you should have a review process where a risk management specialist, a trust specialist that would review those features to make sure that those design principles are really embedded, that they can't be circumvented, that users could be safe, that users can delete their data, that they have choice, and all of those things should then be assured before the product is launched, where what we traditionally see is the engineers and product teams have like a brilliant idea, and they build whatever they want to build, and then they spend so much time building it, and let's say there is some sort of stage gate or a risk assessment process, then at the end, it's like, “okay, wait a minute, this product is launching, but it's missing all of these designs.” So we often recommend truly embedding, privacy, safety and security processes, techniques and design patterns within the whole development process. So that you're just building things trustworthy by design.

Raquel Buscaino: One way to look at this would be, oh, man, I got to cure this upfront investment, but I would even flip the script a little bit because as a consumer, I'm going to only want products that have those trustworthy capabilities, and that will actually, I think, be a deciding factor in many cases, for whether or not I choose a product, so it's less so of trust as an afterthought and more so: “how do I bake in and instill trust from the beginning that way It's a competitive advantage in market, because I know this is increasingly an issue that users, end users, consumers are concerned about?”

Tanneasha Gordon: Spot on, spot on. We're often having conversations with executives and boards on how trust is a business imperative. We're even seeing some companies go as far as like changing the name of the Chief Security Officer to the Chief Trust Officer. So we're seeing that the concept of trust is starting to be understood, and that these disciplines, like privacy, security, and safety, aren't just obligations that you need to just check the box. It's literally a business imperative. You're not going to rely on the product, or have confidence, or feel emboldened to share information if you can't trust that they have implemented some of these guardrails, and we always say, in my team that in today's environment, trust is the crucial currency that companies need to engage customers in in exchange for their loyalty, attention, and business.  It's now a new currency. And what do companies get in exchange for that? Customer loyalty, customer attention and engagement, or just business.

Raquel Buscaino: Well, we've chatted through quite a bit on the episode, and trust is a pretty complicated thing, but when you think about the future, what is something that really makes you excited about where this is heading? Anything in your work, or that you're seeing clients start to see? I would just love to hear from you as we wrap up here.

Tanneasha Gordon: What makes me excited is just to see how human interaction and human relationship with machine works and how these technologies and products can be used in a creative way to our existence, in our work life, in our daily life. So that's exciting.

And I'm also pleased, maybe not excited, that companies are starting to think about this more holistically. I'm starting to see companies actually move from just standing up corporate compliance programs as focused on just litigatory and liability, risk and antitrust and anti-money, laundering like corporate level compliance, and

about the risk to the company. And now they're starting to think about risk to products and start standing up true product compliance organizations that are focused on building trustworthy and high integrity products.

So I think, the especially in the tech sector, it's starting to move in that direction and users are becoming a little bit more aware but I do think more awareness is needed, which is why I'm so delighted to do this podcast with you.

Raquel Buscaino: Well, Tanneasha, I can think of no better way to end trust is really a business imperative. I feel like I learned a lot. So thank you for coming on and sharing your perspective.

Tanneasha Gordon: Absolutely thanks for having me.

Raquel Buscaino: Awesome, and to all our tech savvy listeners out there. If you enjoyed this episode, please share and subscribe, and if you'd like to learn more about how to create trust in digital products. You can follow myself and Tanneasha to stay up to date. Our socials are listed in the episode description. Thanks for tuning in, and I'll see you on our next episode. Until then. Stay savvy