

## THAT MAKES CENTS



### The thing about consumer data

**Host:** Bobby Stephens, principal, Deloitte Consulting LLP

**Guests:** Jon Stine, director, Open Voice Network

Rob Goldberg, Cyber Risk leader, Retail, Wholesale & Distribution, Deloitte & Touche LLP

**Bobby Stephens:** Welcome back to That Makes Cents, the show where we cover the latest trends in the consumer industry. This episode, we're talking consumer privacy. If you've ever gotten a really, really specific ad after texting or speaking to someone about that product and ask yourself, "Wait, is my phone hearing this?" or "Is my smart speaker spying on me?" you'll definitely want to keep listening.

Today, I'm fortunate to have two industry leaders help me unpack these concerns. Our first guest is Jon Stine, director of the Open Voice Network, which seeks to create a future for AI-enabled voice that is standards-based, interoperable, and data-protected, and our second guest is Rob Goldberg, Cyber Risk leader in Deloitte's

Retail, Wholesale & Distribution practice. Welcome, Jon. Welcome, Rob. Thank you for being here today. I'd love to just kick things off by allowing each of you to share a little more about your background and your work with our listeners.

**Jon Stine:** Bobby, this is Jon Stine, and it's a pleasure to be here and, Rob, to be working with you. The background—15 years in the retail industry, followed by another 20 years in the technology industry, Intel and Cisco specifically.

And then Open Voice. In 2016, conversation with colleagues at MIT and in the consulting business, and we talked about what is going to most reshape consumer behavior? What's going to most reshape the industry over the

next many years? And we looked at each other and said, my gosh, this conversational artificial intelligence, this whole technology of voice could be truly a game-changing technology coming to all consumer-facing industries. And so from that led conversations, which is now leading to the launch of the Open Voice Network.

**Rob Goldberg:** Great, and Bobby, Jon, I'm also very pleased to be here with you today. So I've spent my 25-year career helping companies manage risk around IT, cybersecurity, privacy, and I also spent several years as the head of technology and e-commerce audit for a very well-known global retailer.

At Deloitte, I'm helping consumer-based companies tackle these issues in a world that continues to change as we become more digital, more automated, and very, very reliant on technology and data. And so, I spend most of my time working with our clients to help them frame up, in business terms, how they need to think about operating now and in the future to best position themselves to build the kind of trust that's required for them to succeed.

**Bobby Stephens:** Thank you both. Let's jump right in. So I'd like to really start by setting the scene a bit. I think as consumers, we feel like we're hearing about companies experiencing data breaches and about compromised personal info, frankly, every day. But the actual stat is really astounding. In fact, one in every three US consumers has been exposed to some type of data breach. I'm quoting a recent report you authored, Rob. So really what I'd like to do is look to you to just give a little more information around this stat and what's going on with privacy in the consumer and retail space.

**Rob Goldberg:** I think, first and foremost, what's led to this really rapid increase in exposure has been around digitization of business. We're no longer operating in a world where when you go shop at a store, all of the records associated with that transaction and your interaction with that store are sitting on either a piece of paper or some type of manually recorded device. It's all digital.

And when you couple that with the changes in the technology landscape, specifically around things like cloud, you're talking about a large expansion of both the collection, use, generation, sharing, and operational movement of data for businesses to run and to compete in kind of this new era. And so, as a result, what we've seen is that just in the past few years alone, an exponential increase, from retailers in particular, recognizing the value of the data that they hold, even when it's just operational data.

All of this creates value for them to be able to figure out, "How do I get closer to that customer? How do I create competitive advantage by building a stickiness with that

consumer, with that customer, so that they develop brand loyalty to me?"

And so the mere volume of this data that's being collected and used has increased—let's call it the attack space—for those looking to monetize or gain some value by compromising it. So this is really kind of the backdrop of recognizing that data, fundamentally now, is almost equivalent to cash. It has monetary value that can be monetized by bad actors. That's where their focus is, and therefore they focus on retail because retail is generally generating a whole lot of data.

**Jon Stine:** I think he made a very important point about the shift in attitude. Far too long, retailers may have looked at data security as this kind of necessary evil, this cost that had to be dealt with in kind of a compliant way. But now, seeing data security and data use as an extremely important differentiating point of strategy and competitive advantage.

**Rob Goldberg:** Yeah, absolutely right, Jon, and I think what's driving a lot of this is the fact that we now have tools and capabilities that are affordable for retailers to leverage that we didn't have even 10 years ago.

Think about the ability to, for example, recognize someone when they walk into your store by using facial recognition, or be able to tell who's actually on your website simply by the way . . . what they click on and what they look at, without even being logged in. And so you see much more activity around very personalized marketing. Using tools like location tracking, visual search, and even, as I know we'll talk about a bit, voice capture and leveraging the voice, really satisfying the needs of the customer, as well as the needs of the retailer. So all of these things have kind of changed the game in terms of how retailers operate, and therefore what they're collecting and what they're using, which opens up risk when we talk about privacy.

**Jon Stine:** And Rob, I think you also make another great point here and ought to be emphasized, that the whole issue of risk and security to a degree becomes expanded. There is the risk of a data breach,



for instance, but there are also—and especially with CCPA, GDPR, all the changes in legislation and regulation—issues of data usage also become part of that security question, perhaps, and it really seems to be a new era of data security for retailers.

**Bobby Stephens:** So, Jon, every one of my clients in the last year or so has really asked me about CCPA, what it means, even those that don't have any sort of operations in California. And really, it's a big question that's out there. It's sort of one of those things that has been looming, and now it's here. So now that it's here, what are the things that we need to worry about now, and what are the things that are more "wait and see?" I'd love to hear both of your perspectives on that.

**Rob Goldberg:** I think, first of all, companies obviously need to be in a position to be able to respond to requests from consumers about what data they hold and be able to satisfy requests regarding the deletion of their data upon a verified request. The biggest challenge is knowing where that customer data is, where it's going, how well it's protected.

So today, retailers need to first and foremost make sure that they can be compliant. Although in most cases, and what I'm seeing, that's requiring a lot of heavy lifting, a lot of manual effort, in order to achieve those targets. Longer-term, that's where retailers should be looking to, evaluating how they want to operate, how they want to interact with consumers, how they do it today, but more importantly, how

they're going to do it. And start to work on those things with privacy by design, thinking about, for example, processes in the store actually involving and engaging folks in operations and merchandising to have the privacy discussion on the impacts of those operational decisions, so that in the future, becoming compliant with privacy law is not a closed-gap exercise, but it's really a matter of simply tweaking operational processes and technologies that were designed with privacy as a design element.

**Jon Stine:** I'd echo what Rob just said, and I think he used the great phrase, "privacy by design," and quite simply this is something to be taken, number one, very seriously, and number two, to understand that you can't just put a Band-Aid on this and tell your board and look around and say, "Hey, we're okay."

**Rob Goldberg:** And if I can refer back to kind of the study, the survey that we did of over 200 retail executives, one of the things we saw coming out of that study was that there's a definite bifurcation in terms of organizations' approach to privacy. We've kind of grouped them into a couple of different groups. One being leaders, so to your point, Jon, you know, the leaders are the ones who really are thinking about privacy as a strategic element of discussions happening in marketing, happening in merchandising, in store operations, in e-commerce, digital, mobile, etc. As opposed to what we've called the laggards, are ones who are largely focused on having that discussion with the general counsel and with legal to say, "How do we make sure that we can show a regulator that we're compliant?"

There's a wide range of organizations that fall in the middle, which are the ones that we're calling adopters. Those are ones that might have a cross-functional team that discusses privacy, but it's not yet at the strategic end of how that retailer operates or how they will operate. And so that's where we see kind of the natural progression that needs to occur.

Retailers like to talk about personalization in terms of being able to satisfy me as a shopper, that I'm going to get the type of

curated experience that's tailored to my preferences, my color preferences, size preferences, etc. But what we also have to remember is, there's also attitudes to how I like to be interacted with and whether something you do might cross that imaginary or invisible line of the creep factor with something you might do with my data. And so if organizations . . . If these retailers are truly thinking about privacy as a strategic element of their business, they're going to be able to really personalize that experience so that they never cross that line.

**Jon Stine:** When you boil down the term "personalization" in retail, at the core of that is less about massaging a specific message to a consumer, it's about trust. I trust you, the brand, that you will use my data in a way that benefits me, that respects me, that recognizes me, that rewards me. And so that trust is that red-hot gravitational core that makes personalization work and makes the relationship between brand and consumer valuable. It's a great point, Rob.

**Rob Goldberg:** I love what you just said, because I don't think we talk enough about trust in the industry. We know how hard it is to build, and we know how quickly we can lose it. I haven't seen a lot of discussion of tying trust to the privacy topic, to be very frank, and I think that that's something that resonates from a business point of view. So if you can have a trust discussion instead of a privacy discussion, I think the points you just made, Jon, can help retailers shift that conversation to a more business- and strategic-oriented one and kind of stay away from that trap of being a laggard, where you're primarily talking about privacy as a legal issue.

**Bobby Stephens:** Guys, I think that's fascinating, that the sort of symbiotic relationship that has to be created between the data sharer and the data, the holder and the user of the data, is really important. There can be great value to both sides of that it's done in an effective . . . And I like the word trust versus private or safe or any of those things, because it really is a trusted sharing of that responsibility to make it easier, faster, whatever for the consumer and more profitable and driving growth and business value for the company itself. But as we switch gears a bit, and thinking

about the specific kind of data that will fall under CCPA as it continues to roll out, not just in California, but likely other places here in the US, I really think that probably most consumers and people, retail executives know a lot about today's data. You have basic profile and preferences, purchase history, browsing history, location tracking, etc. But I would venture to think that fewer people directly associate voice and consumer privacy. So, Jon, would love for you to tell us a little bit more about voice technology, and let's start first with some of the cool things it can do and how it's evolving, and we'll talk about the scary parts later, but let's start with cool stuff first.

**Jon Stine:** Well, man, Bobby, voice, just by its very nature is the easiest, simplest, most convenient way to communicate with the Internet, with a brand, with the smart home environment or the smart environments. Some people call it the zero interface. When we're born, we're not typing or tapping or swiping, we're talking. And it is a rapidly growing area of availability and adoption. People are using voice in so many different ways. You know, there was a study recently from Voicebot on 2019 data, that some 25 percent of all smart speaker users are using it to research products. Google sent out some information, and Voicebot did some estimates, and we anticipate that one in eight, maybe closer to one in seven now, overall Google searches are done by voice.

**Jon Stine:** Voice is also a biometric identifier. With some high-90s percent of accuracy, by a study of our voiceprint, we would be able to identify Bobby, Rob, or Jon.

Also, and interestingly, that MIT studies have shown that sometimes, physical or mental illnesses could be diagnosed by voice, such as Parkinson's, certain signs of schizophrenia can be identified by voice. And then also sentiment analysis. You can identify confidence or lack thereof, hesitation, all kinds of things that can go into understanding shopper behavior and attitudes, yet giant questions about how do we use—especially as voice enters the realm of commerce, as we come into this age of conversational commerce—how will we use this data? What will be our ethical guidelines? What will be our standards? How should—to Rob's earlier points—how

do we manage, store, filter, anonymize this remarkable set of data?

**Rob Goldberg:** Well, and Jon, let's face it, we love it. I love it. I love the tools that are available to us now using voice that just make life easier. I love being able to say to my television, "Tune to channel X." Now, obviously that's the ultimate in laziness, right? I can't even pick up the remote anymore because it's just too easy to say, "Hey, I'd like to watch this program," and it just happens.

I do think that it comes back to, though, some of the things we were talking about earlier on that personalization aspect and trust because, if I reflect on kind of my wife's use of this technology, it's much more muted than mine. She rarely asks the device questions, even with my encouragement. Even in our own household, there's a wide range of both acceptance and trust of voice technology and, therefore, as use. That has a number of implications for, for example, retailers who are looking to leverage this type of technology for their own benefit.

**Jon Stine:** There are a number of very important questions, which the industry and the organization that I'm leading, the Open Voice Network, will need to address and answer in the coming years. And as we see an entire shift in the retail industry toward a value proposition less about the four P's of tradition and much more about ease and convenience, the ability from your kitchen to simply say, "Reorder. Ship it." It doesn't get easier, and certainly for the consumer, it doesn't get better than that.

**Rob Goldberg:** As you're talking about that, I'm thinking about my, one of my 13-year-old twin sons, when I'm not home, saying, "Order an Xbox," or, "Order the latest game," or whatever. And I don't want that to happen. So there are things about voice that, I guess, I have concerns as a consumer about that kind of play into what you're talking about there.

**Jon Stine:** Issues of identification or authentication. Who should have the right in Rob's household to order the Xbox? Who should have the right in Jon's home, in Jon's kitchen, to order the additional wine or

beer? Major issues, Rob. Absolutely. And the issues of bycatch, what it's termed, as well as just the protection of minors, very important, need to be addressed and certainly within our work and pursuing standards within voice, the kind of questions that we are planning to address and bring to either ethical guidelines or recommended standards.

**Bobby Stephens:** So I think you guys hit on a lot of really interesting points, especially from the consumer side. And, you know, the voice technology is here in pockets, and Rob, you mentioned, right, even at your own house, you and your wife using it quite differently and adopting it in a different manner. So, you know, we probably have a few years to still figure out exactly what needs to happen here, but that's not that long in the scheme of things. How do you think enterprises, anyone, retailers, of course, consumer products companies, you know, ad services, anyone who's collecting voice data and dealing with this new set of information overall, what are some key things that they have to start thinking about to protect people's privacy and vis-a-vis really provide that trusted and safe experience for the end consumer?

**Jon Stine:** I would say it starts, Bobby, back to Rob's earlier point. It starts with privacy and proper data use by design. If you take that overarching strategic view, then you'll be working at various levels on data security. You'll be working to respect how data is used within your artificial intelligence processes. You'll be understanding the implications of biometric identifiers, be it voice, be it facial, however that is. And so working at multiple levels, but all around the core of the dignity of data, the respect for data, and privacy and security by design, that will take you in the right direction. Now, that's a very broad statement, but I think an overarching, broad approach will be necessary. Rob, your thoughts?

**Rob Goldberg:** Yeah, Jon, I completely agree with that. I think that organizations don't . . . Retailers don't necessarily have to do anything fundamentally different than what they should already be doing, to be very frank. I mean, at the end of the day, voice, in

terms of how it's used and how it's going to be used by retailers, it starts with an analog signal, it's sound, but that gets converted at some point through, you know, some type of a receiver, microphone or otherwise, to digital data.

So in terms of thinking about voice as data and expanding perhaps their thoughts around how that data could be used, monetized, or leveraged in some way, that's where retailers need to focus. Because, as Jon pointed out earlier, you have situations where you can learn a lot about a person just by listening to their voice, not even necessarily listening to the words they're using. There's value in . . . let's call it voice metadata. And Jon, I don't know if that's the right term, but it's what you can infer from the actual sound of a person's voice that also contains rich data as a very valuable and potentially dangerous asset if it's misused, if it's lost or stolen, or if it's held on for too long.

I've seen a lot of organizations, through this whole California Privacy Act exercise, struggling with the data retention challenges, because they just haven't thought about it before. How long should we keep calls to the call center? Those voice recordings. How long should we keep this information about a customer who has not interacted with us since five years ago? These are all fundamental issues and questions that need to be answered now about a new type of data that, while it is data, also is different than traditional data that's computer-generated.

**Bobby Stephens:** Why do you think we need to care about having standards around this, and what would be your interpretation of what some of the standards around voice might really be?

**Jon Stine:** Bobby, I think there's several areas in which the voice environment is crying out for standards. And I might suggest that voice is kind of in the same place that the Internet was a number of years ago back in the Explorer and Netscape days, and that Wild, Wild West of proprietary walled gardens and before the Internet truly became interoperable. I think there are the four to five areas in

which the Open Voice Network and our sponsoring and member companies are pushing. And one would be just having a destination registry, a DNS for voice. Another, and something that we've talked about here, is guidelines and standards on identification and authentication, protecting children, assuring parents, other things such as just the commands and making it easy for developers and enterprises if we had a standard set of commands for transactions, for instance, and then issues of data privacy and guidelines on data use, and then certainly the issue of interoperability across platforms. Rob, to you.

**Rob Goldberg:** Yeah, Bobby, I think what's happened so far, particularly around voice and really around technology in a lot of ways is, a few big companies have created an opportunity for us to see what's possible. But most of those opportunities are proprietary, and they're enclosed systems, which means that if you want to play by their rules, that's how you get to play. And, of course, that can limit opportunities for growth.

On the standards side, I think, you know, it's easy to complain, but we also have to be honest about how we got there. And the fact of the matter is that, in particular in the US, we, as you know—and this is a very general statement—but we've been fairly cavalier about privacy. Whereas, you know, other countries, other markets have always kind of had privacy as a top-of-mind issue. So I think there's both a need for, on the standards for voice, for example, opening up so that more of industry can benefit and we're not locked into one or two proprietary ways of leveraging voice. And then on the regulatory side, we need to engage with legislators actively and proactively and with consumers to really understand what's important to them. Again, back to personalization, so that we don't have future regulation pushed down on us because of a failure for us to self-regulate.

**Jon Stine:** Let me echo that. It's a truism that standards will emerge regardless of what we do. Now those standards—if we do nothing as an enterprise community—those standards could be imposed from above through government regulation. Or if we do very little, those standards can be imposed

by major proprietary players. What we're suggesting here to the work of the Open Voice Network is the enterprise community coming together to propose standards and ethical guidelines, usage guidelines, that will work for the many.

**Bobby Stephens:** So one fun question. We talked a lot today about the risks of tech-enabled retail, but there's obviously a lot of value to it. And so if I asked you to just take a step back and just imagine what would be the coolest or most amazing thing that a retailer or consumer products company could do to make your life easier and better as a consumer, what comes to mind?

**Jon Stine:** I'm very excited. If you take a look at the intersection of AI, voice, and advanced thinking and technology, it'll be two to three, three to five years, and I will have a digital twin doing shopping on my behalf and interacting with my favorite brands, who will come together in federations and serve as my lifestyle concierge. From travel, to groceries, to pharma, to this, to that. The potential for a future of true ease, convenience, and value on both sides. Me and my digital twin working with brands that I trust.

**Rob Goldberg:** I travel a lot for work. I'm away from home. Today I'm up in the Northeast. You know, my wife and I were talking this morning, and she says, "Hey, do we have any coffee?" And I said, "Well, what do you mean? I just left yesterday, and there was coffee in the machine." And she said, "Well, it's empty," and I said, "Well, I usually keep an emergency stash in the freezer. Check there. Did you check there?" She said, "Yeah, I did, I don't see any." So if I just use that very simple kind of real-life, everyday example of, you know, we ran out of something.

I am excited in a future where either during that conversation, if my privacy preferences allow it, the retailer can pick up that I need coffee, and they already know what type of coffee I like—that it's organic, it's whole-bean, it's espresso roast—and that within an hour, it's at my house, that will have removed a whole lot of friction from my life. But that's not the only channel that that could occur

during a real-time conversation with my wife. It could be that I hang up with my wife, and I simply say, "Hey, we need coffee at home," and within an hour the coffee that I buy is at home. The ability to almost have real-time fulfillment of the things I need, which completely remove friction from mine and my wife's relationship because I was the person who normally buys the coffee, and I obviously failed in this case. So a retailer that can help me avoid those issues in the future will be one that I am very loyal to.

**Bobby Stephens:** Well, I think I'm possibly buying both of those. And frankly, I think we can all see in our daily interactions today, you know, logical and viable places where those could fit in if done correctly. So, you know, at risk of showing my age, it does sound like one could paraphrase the words of Notorious B.I.G. when it comes to privacy, which is "mo' data, mo' problems." And you look at problems like more attack space, additional liabilities, complex regulations, etc. However, through this conversation today, one thing that I've sort of taken some positive from is, if done right, using your term, Rob, privacy by design and creating and embracing standards, getting out in front of it for new data like voice, Jon, feels like we could create a trusted and valuable relationship between the data sharer and the data storer here now and in the future.

So I'm excited about that. I really appreciate you both sharing your knowledge, Jon and Rob, really great stuff. If any of you are interested in learning a bit more about consumer privacy in retail, check out the [report](#) that we mentioned earlier, coauthored by Rob. You can just visit [Deloitte.com](https://www.deloitte.com) and search "consumer privacy in retail." That's all for this week. See you guys next time on That Makes Cents.

You can listen on your favorite podcatcher, whether it be Apple podcast, Stitcher, or Spotify. Simply search for That Makes Cents. Connect with me on social media: Bobby Stephens on LinkedIn or @bobbystephens on Twitter.

## Learn more



Visit the That Makes Cents library:

[www.deloitte.com/us/that-makes-cents](http://www.deloitte.com/us/that-makes-cents)



Join the conversation on Twitter

[@DeloitteCB](https://twitter.com/DeloitteCB)

This podcast contains general information only and Deloitte is not, by means of this podcast, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This podcast is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this podcast.

### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.