Transcript Episode 14 Cosanna Preston-Idedia

Ron Kruzeniski:

It is my pleasure this morning to be talking to Cosanna Preston-Idedia. She is the Vice President of Digital Identification Labs of Canada. And I'm going to start by first asking you, Cosanna, to tell us a bit about yourself and how you got involved in the whole area of digital ID?

Cosanna Preston-Idedia:

Sure. So yeah, it's the Digital Identity Laboratory of Canada. It's a mouthful. So we can say IDLab for short. That's no problem. For myself, how I got into ID, specifically tech in general, it's a bit of an unusual career path. I always tell people I started in social sciences, so my degrees are in political science and African studies, and spent my early career in non-profits, a bit in academia, quite a bit of time in communications, public relations, but with every job, and this would've been the early 2000s, 2010s kind of thing, as technology was becoming more and more prevalent in the workplace, specifically digital, the internet, those sorts of things. The tech part always seemed to be on the corner of my desk. So, I helped consistently design websites or startup social media offerings at an organization that I was at. And gradually, that became more and more a part of my job, which I think is pretty typical for people who were in university in the late '90s and early 2000s.

So as that became more and more part of my job, eventually, I found myself at the Government of Saskatchewan in the IT Department, working on digital service transformation, and we recognized that digital identity was the next thing that we needed to be focused on. I have a track record of being able to carve out new paths. So, I took on that challenge of trying to figure out what a digital identity program could look like for the Government of Saskatchewan. Fast-forward to 2022, and the government made a decision to pause that program. And so that is when I took the decision to change organizations and I'm now with the IDLab.

Ron Kruzeniski:

So, as we get into this, definitions become important. And for our listeners, I'm going to say to you, what is digital ID? And I hear often the phrase, "Digital credentials." What do those two terms mean to you?

Cosanna Preston-Idedia:

Yeah, absolutely. So digital identity or digital ID is the first common term that I think people have gotten used to. And digital credentials is maybe a newer term, but really, what we want to think about is our physical documents. And I'll explain the two terms in that context in a second. When we think about our day-to-day life, we have a number of important physical documents. Some we use on a regular basis like our driver's licenses, and others we may use on a less regular basis like a university diploma or a transcript or a birth certificate, a marriage certificate. All of these are important documents that have different ways of defining things about us, that we went to university, that we're married, that we were born, we might have notarized documents, we might have professional association documents that prove that I'm a doctor or a lawyer or what have you.

So all of these, we can loosely call our credentials and we have used that term with physical credentials for quite a long time. What we're trying to do in the digital space is say, okay, how do we take those physical documents and use them in the digital way that we can trust that the document is the right document, that we have confidence that we're showing it to the right person? And that's really what digital identity and digital credentials are trying to do. So when you think about digital identity, if we think about all the situations in our lives where we're asked for government-issued photo ID, and that's

effectively what we're trying to do is create the digital equivalent of a government-issued photo ID. And when we think about digital credentials, it's that whole suite of important documents that define different aspects of who you are and making those digital.

The challenge is today is we would probably all know extremely well, it's very difficult to use our physical documents digitally. So it might mean taking a picture of something and emailing it in. It might require a fax machine and how many of us have access to a fax machine these days? But ultimately, we're trying to do things like get access to health information. Increasingly, employee processes, hiring processes are online. We want to be able to sign major contracts, certify important documents. I think about engineering stamps, do major financial deals. We should be able to do all of that online, but we're constantly pulled offline because we need to rely on these physical important documents.

And so to be able to put that online, we want to know that the people that we're interacting with are legitimate and they're the right person. Right? Because you need to know. That's an important private document to you. You need to know that it's going to the right person. You want to have confidence that there's nobody who is a bad actor. So somebody who has bad intentions, who's getting involved in the middle and you might not know. So that's our security side of things. And ultimately, we're here. This is a privacy conversation. We want to make sure that we're only sharing the information that is needed for that transaction.

So, a really common example in a digital identity space is today, if you're trying to purchase alcohol or enter a bar, you might have to show your driver's license or another type of government-issued photo ID. When you hand over that driver's license to the clerk or to a bouncer, they see your full name, they see your address, they see your birthdate, your height, your eye colour, they don't need any of that. All they need to know is that you're above the legal drinking age for that province. So 18 or 19.

And so what digital credentials are starting to do is just try and show us that only that specific information, rather than a handing over my life story to the bouncer, I can just show them proof that I'm 19 and above, for example. So I hope that comes back to a digital ID, is the government-issued photo ID equivalent or any sort of identification document like an employee badge. Digital credentials is that broader spectrum of those important documents that define different aspects of your life.

Ron Kruzeniski:

So, there's lots out there in the media talking about digital ID, but what's your assessment of the current state of digital ID affairs, first of all, internationally, and then more specifically in Canada?

Cosanna Preston-Idedia:

Yeah, there's lots out there right now. And like anything right now, digital identity, digital credentials are bombarded with a lot of misinformation and some active disinformation, so some active attempts to provide incorrect information. And so it can be hard and it can be scary, and there's some pretty scary scenarios presented out there. So I really encourage people to always look to reputable sources, things like DIAC, the Digital Identity and Authentication Council of Canada, and various other sources, including provincial governments, the UK, New Zealand, Australia, many European countries, they're all working on digital identity and are good sources of information.

They're also good sources of information because these are jurisdictions, countries, states, provinces that are working in a similar way to how the conversation is unfolding in Canada. So in Canada, we're very focused on privacy-protecting, secure, easy to use digital credentials. That is not the case in every part of the world. I would say the UK is working that way, New Zealand, Australia, European countries and a number of others, but the reason that there's a bit of fear out there is because there are other countries, and the most common example is China, that is not focused on a privacy-protecting secure

digital identity. It's a more centralized approach. People may have heard the term, the Chinese Social Credit System, and I know that's come up as something that people are quite afraid of in Canada.

And so it's really important to understand that not all digital identities and digital credentials are the same. Different countries are going to implement these programs in different ways, and the key focus in Canada is really four pillars that we often talk about, that it's privacy-protecting, first and foremost. That means your data is in your control. That it's secure. So that's that bad actor thing we were talking about earlier, you know who you're presenting your data to, you know you can trust them and there's nobody in the middle who has bad intentions. That the digital ID is easy to use. We have all been on websites and done digital services that are really hard and frustrating, and we've all been on the Amazons of the world that are really easy to use. And there's no surprise why websites and apps that are easy to use are more often used. So it's really important that our digital identities are easy to use, our digital credentials are easy to use.

And the fourth pillar is equitable access, which really boils down to anybody who wants a digital credential should be able to access one. And notice, I emphasize want. So my belief, and I know that the common belief in Canada is that digital credentials should be optional, they should not be forced on anybody, but anybody who wants one should be able to get one. And so what that means, and what that's increasingly meaning in Canada and other jurisdictions that we've been talking about is if people maybe don't have consistent internet access on their mobile phone, is there a shared computer they can go to in a library or a friendship centre or some other community organization where they can still access those digital credentials, where they're not prevented from accessing a digital credential because of their socioeconomic circumstances?

So that's the framing that we're seeing in Canada and in, I would say like-minded countries across the world, but it is really important to remember that not every country is working on this in the same way. And so if you hear something scary about digital identity, maybe pause and see, is that country specific? Is that true information? Is it coming from a reputable source? And how do I ask more questions to get a better understanding about it?

Ron Kruzeniski:

So, you've touched on some of the pros and cons of digital credentials, and if you have other pros and cons, please elaborate, but I guess are we as citizens missing out on anything by not having a digital credential system?

Cosanna Preston-Idedia:

Yeah, so I think it's important to know, first of all, the way we talk about digital credentials now suggests that it hasn't been around. And Alberta and BC, for example, have had digital credentials, digital IDs for a number of years now. So digital ID in itself is not new, but those systems are centralized systems and other provinces are experimenting with what we call decentralized systems. So, when we look at pros and cons, the best way to describe a decentralized system is to come back to our driver's license, again, in that example we were talking about. When SGI, our driver's license issuer, if you're listening from outside of Saskatchewan, issues you a license, they have it on record that they've issued you a license. So, SGI knows that Cosanna Preston-Idedia has a license, but they don't know how I use it on a day-to-day basis. So, every time I pull that license out of my physical wallet and present it to somebody, SGI has no idea that's happening.

Up until very recently, we haven't had the technical ability to do that with a digital identity or credential. And so you see what we call federated uses of digital ID. And so that might be you're logging into government site to access government services and you're using one username and password and it's all

connected. Right? You've had to go into a site to identify yourself, and then access a service. With the decentralized approach, the pro there is that we're now able to use our digital credentials in a way that is more privacy-protecting. So again, only I and the organization or person I'm sharing my digital credential with know that it's been presented, and it offers some of those protections that we were talking about where I don't have to show my full birthdate. I can just show that I'm 19 or over.

So while we see a lot of criticism and concern and fear around digital credentials that the government's going to know everything about you and they're going to be able to know exactly how you've used all your credentials and that this is state surveillance, it's actually the opposite in the Canadian implementations that we're seeing roll out across provinces, and it's important to know that it's province by province, right? It's not one digital identity system for the whole country. It's not a single database. Right? We talked about different documents. So the universities would be in this digital credential space, universities would be responsible for issuing university documents. Governments would be responsible for issuing standard government documents.

So it's decentralized in that way, in the way that the person who issued or the organization that issues you physical documents issues you digital documents, and it's more privacy-protecting because you have more control over your data than you do today when you send in a photocopy of your ID to somebody's email and you don't know how they're storing it or who has access to it and how that information is used after you've sent it across. So, there are some real benefits to this shift, to this decentralized approach.

Ron Kruzeniski:

And are we missing out on anything if we don't have one?

Cosanna Preston-Idedia:

I think what we're missing out on is access. So let's take cash as an example. Right? When we only could pay with cash or cheque, you had to physically go to a person and hand them that legal tender, that cash or cheque. Once we got e-transfer and the ability to pay online, and now it's even Apple Pay and all these things, suddenly you can purchase something without having to be physically there in a much easier way and in minutes. Right? We order on Amazon these days all the time because we now have these new methods of payment that allow us to do so digitally. So it's increased our reach, it's increased our ability to interact around the world, and digital credentials offer that same opportunity. Whereas before, you might have to get a physical document notarized, and then mail that document over to a different province or a different country or what have you.

And that whole process of the notary process and then putting it in the mail and them receiving it and processing that physical copy can take weeks and months. If we can do that digitally, you don't need to have that notary step because the digital document is authenticated. There are technology processes in place to confirm that yes, this is a valid document. You can present that document to somebody across the world within seconds. And so it speeds up our ability to interact in the same way that payment cycles have been sped up. When we're missing out, it means that any jurisdiction that has that digital credential capability, the people in that jurisdiction are able to move faster and with greater ease than the people who don't have it.

Ron Kruzeniski:

Should Saskatchewan have a made in Saskatchewan digital ID or should we rely on others to come up with something that we then can use?

Cosanna Preston-Idedia:

Well, and so if we think about the split between digital IDs and digital credentials, and we look at what Saskatchewan's responsible for, the Saskatchewan government through SGI issues driver's licenses. So if we're talking about government-issued photo ID, we can have a digital copy of that. And in the same way that SGI is responsible for a physical driver's license, it follows in my mind that they should be responsible for the digital version of that document, that we wouldn't bring in a private company to start doing that, that SGI would continue to be responsible for that digital version. When we look at the Government of Saskatchewan, you can think about the government issuing things like permits, all sorts of different types of permits and licenses and those sorts of things. And to me, it follows that if the government is currently issuing those physical copies, that they should continue to evolve that process to issue the digital copies.

So yeah, I do think that Saskatchewan should be moving in that way. I respect the decision of the government to have paused the program. That's the prerogative of the government, but I do think just like debit cards weren't an if, they were a when, when they started coming, and debit cards today remain optional. You don't have to have a debit card, but many, many, many people have chosen to use the debit card because they recognize the convenience and benefits that it offers. I do think we need to start shifting that way with our digital identification and credentials to enable people to make that choice if they want it.

Ron Kruzeniski:

So, I've heard certain announcements and have you picked up any interest in large tech companies, maybe not in Canada, international actors getting involved in the whole idea of providing a digital ID?

Cosanna Preston-Idedia:

Yeah, absolutely. The most common, if people, again are looking for information and you're Googling these things, one of the ones that you'll probably come up on is Apple providing mobile driver's licenses is what it's called, or MDL, but we can just think of that as a digital driver's license, to a number of state governments. In some ways, you can see the convenient factor. A number of people have Apple wallets already and keep their credit cards in their wallets and concert ticket and airline tickets and all sorts of things. So we know it works. Right? And so follows like, "Well, why wouldn't I just put my ID in there?"

The challenge is that once Apple has that... There's a couple of challenges with that. The first being that we've been talking today about a whole spectrum of digital credentials. These examples that were coming out in the states are presenting themselves as, "We've solved the digital ID problem," but really, it's just solving a problem for a very specific credential. Right? The driver's license. So it doesn't address the whole realm of credentials that we ultimately need to address. That's one.

The second thing is that it's a mobile-only solution. So we've talked about today that a critical pillar in Canada is around equitable access. Anybody who wants one should be able to get one. If it's mobile-only, that means people who are already pretty disenfranchised in our province or in our country will be further disenfranchised because those are the people that depend on library computers, friendship centres, band offices, et cetera, for access to the internet. So mobile-only won't serve them. So we risk creating a greater digital divide, and we're already seeing digital divides in our province, in our country. It's my firm belief that we don't want to contribute to that digital divide. So it's another challenge with Apple in that approach.

Then the third challenge becomes more philosophical, around to what extent do we want private companies controlling our government-issued photo IDs? And that's a debatable topic. I have my personal opinions on that topic, but an important thing to remember is that once a private company

takes over that responsibility, they make the decisions about the privacy, they make the decisions about the security, they make the decisions about the business model, and Apple's a really big company. Each state will have to negotiate specific terms, and that can get pretty complicated pretty quickly. And it's not always transparent to the citizens, how those negotiations are happening, what the specific terms are. So that's something that I think we have to be really mindful of as well.

Ron Kruzeniski:

So final question, Cosanna, what can organizations do now to advance digital credentials?

Cosanna Preston-Idedia:

First and foremost, organizations probably feel like, "Oh man, this is new tech," because it is. "It's still evolving tech and how do we get involved? And we're not very techy and we don't know what to do." The first thing to do as an organization is to understand what role you need to play in this ecosystem. So as an ecosystem, you might... I'm just trying to introduce terms so that if people are seeing stuff online, they know how to start. So you might hear the term digital trust ecosystem, and digital trust ecosystem is just a way of explaining that there are a number of different rules to be played. So let's use an example again. Let's take a credit card. We have issuers of the credit cards, MasterCard and Visa, but then they delegate those abilities to different banks and that kind of thing. So that's a whole part of the ecosystem, is the issuers.

Then you have the holders of that credit card. So if you have a credit card, you keep that credit card in your wallet, you are the holder. You have a wallet that in this case, in a credit card case is typically a physical wallet, but Apple Pay. Right? There's now e-wallet. So that's a piece of the ecosystem. And then you have probably the most common piece. So for individuals, your role is probably just to be a holder and to decide if you want a digital credential. And if you do, how to get one. If you're an organization or a government, your role is probably an issuer or the third area, which is called verifier. And so verifier, if you think about credit cards again, when you go to a store, you present your physical credit card and you tap it or you insert it into a point of sale machine.

And so businesses have to make a decision to accept credit cards, and if they're going to accept credit cards, they need to enable their business to be able to accept credit cards, whether that's online or physically in a store. And to do that, they go out and get a point-of-sale machine. There's a number of different companies. Moneris is a really common one just to help your pin pad, right? So, first of all, the first step is a government organization is identifying where do you fall in that whole digital trust ecosystem? What are you? And as a government, you're probably an issuer and you're probably a verifier. You probably issue permits and government-issued photo ID, and all those kinds of things. But also, when citizens come to you for services, they probably need to present a digital credential or a digital government-issued photo ID to you, and that makes you a verifier.

As a business, the average business, we talked about the alcohol example because it's a pretty easy one, earlier, as a bar or a liquor store, you're going to be a verifier. So you're going to need the technology in place to be able to verify. Understanding your role in that whole ecosystem is the first step. The second step is getting a roadmap in place. And so you are making a decision that, "Yes, I want to participate in this digital trust ecosystem. I want to be able to accept digital credentials in my store, or I want to be able to issue digital credentials to my constituents, to my citizens, whatever that might look like. What's it going to take for us to do that? How do we want to do that?" So that's your roadmap, that's your strategy.

I would really, really encourage people to stay focused on those four pillars that are quite dominant in Canada so that it's secure, that your solutions, your participation is privacy-protecting, that you ensure

that whatever you're providing to citizens, whether it's an ability to use that digital credential or that digital ID in a store or to issue one, that it's really easy for people to do so that if people want one, they can get one without too much frustration or time or barriers, and equitable access. Whoever wants one should be able to get one. So make sure that it's being offered in a way that people with physical disabilities, people who have site disabilities, people who have socioeconomic barriers still are able to participate if they want to. So yeah, I think those are the key things.

The last thing I would say is this is not a short journey. It is a larger journey. It's not overnight. You can't decide today that you want it and you get it tomorrow. So, I think the key thing for governments and for organizations that aren't actively participating in digital credentials yet is start figuring out where you are in that ecosystem. Start figuring out your roadmap because it's a couple of years to success. So if you want your citizens to have that global access in the way that we do with payments today, we need to start now.

Ron Kruzeniski:

Cosanna, thank you very much. You have done a great job in terms of clarifying the concepts, clarifying some of the benefits, and clarifying the risks and identifying the pillars. And I hope when people listen to this, that they have a much better idea of what the whole topic is all about. And as you say, that part in the end is we all just need to get familiar about the subject matter and know what we're talking about.

Secondly, thanks for taking this time out of your busy schedule, and I know you have other interests besides digital ID, and obviously sound like a very busy person, but thanks for taking time to do this podcast today.

Cosanna Preston-Idedia:

My pleasure and thank you. And I would just say, if anyone has any questions, the Digital Identity Laboratory of Canada is a great place to go to start those questions. We've got lots of material to learn more. Right? The critical thing here is reputable information. So, I mentioned a couple of other organizations in the podcast and I'd be remiss not to mention my own. So that's another great place to go for information.

Ron Kruzeniski:

And I assume if people do a Google search, they can quite easily find your organization's website.

Cosanna Preston-Idedia:

That's right. Yeah.

Ron Kruzeniski:

Thanks again.

Cosanna Preston-Idedia:

Thank you very much.