Di **[00:00:31]**: We are so glad to welcome Mike Overton and Maury Mitchell from the CONNECT Project. Gentlemen, may I ask you to introduce yourselves? Mike, tell us who you are and what your involvement with the CONNECT Project is.

Mike Overton: Okay, I'm Mike Overton, with the Nebraska Crime Commission. I'm the Chief of Information Services for the Commission. I've been involved with CONNECT for a number of years as we tried to really establish a data sharing framework between Nebraska, Alabama, Wyoming, and Kansas.

[00:01:01]

Di: That's great. And, Maury, may we ask you to introduce yourself?

Maury Mitchell: Yes, I'm Maury Mitchell, Director at the Alabama Criminal Justice Information Center. I've been there for about eight years. We started the CONNECT Project I guess back in 2007 when Mike and I got together and decided that we were doing some innovative things with technology, and the internet, and sharing information. And, if our states could do it internally, could we maybe do this across state lines? So, we got together with our friends in Nebraska, I mean, Wyoming and Kansas. And ultimately, it led to this project.

Di: That's fantastic. We're also joined today by John Ruegg. And John, in addition to many other hats that you wear, I believe you are the Chair of the Global Federated Identity and Technical Privacy Task Team?

[00:01:59]

John Ruegg: That is correct. So I'm John Ruegg. I'm also, in my day job, the Director of the Los Angeles County Information Systems Advisory Body. I really met these two fellows on the CONNECT Project on a conference call we had about five, six years ago in which our committee, the Department of Justice Global Security Working Group was – at that time – the name of the committee, was really working on adopting standards for secure information sharing across jurisdictional boundaries. And I had the privilege of talking with Maury, who was chairing one of his administrative committees. And we introduced the concept and I've been active kind of with the CONNECT Project on and off over the last four or

five years. So it will be interesting to hear more on how things have progressed.

Di: So one of the concepts that we understand about the CONNECT Project is that it's a consortium today of four states. Could you tell us a little bit about what kinds of data you are sharing across those state boundaries?

[00:03:05]

Maury: Well, today we've got driver's license information. We're working with corrections data and we're working with court data. We've also identified maybe six or seven other areas where we know we're capable of sharing, but we've started off with this data across state lines.

Di: Mike, did you have anything to add to that?

Mike: No, really just started out by trying to identify – it was kind of the classic approach: find a dataset and then try to narrow down data elements that you could share. And we wanted to do something that would have a broad appeal. And that really kind of led us to GFIPM [Global Federated Identity and Privilege Management], and the security, and how we built from there. So we've almost put more things into the technical side, and now we're able to circle back to add more data. So it's been a good process.

Di: What kind of business problems were you trying to solve with this four-state consortium?

[00:04:01]

Maury: Well, when we first started, it was more of a conversation of ***can*** we actually share data? Can we –

Di: Like a proof of concept?

Maury: It was a proof of concept in the early stages. Of course, there were classic ways to share information across the nation through NCIC [National Crime Information Center] and NLETS [International Justice and Public Safety Network]. But those were pretty much fixed methods of doing things. And we found in our own states that we had much deeper reservoirs of information. We could go find great details and even unstructured data deep within the court

system, or within the probation system, or corrections, or driver's license with photos.

And at the time, you were not capable of bringing any of that kind of information up on a national standardized system. But we could do it within our own states. So we decided, "Can we possibly connect our own versions within our states with each other?"

[00:05:03]

But we did not have a game plan about how to go about it; it was more of brainstorming session. And about this time, the Global committee was coming up with some national standards and it just fit perfectly with us saying, "Well, wow, let's take a look at these and see if we can adopt them and prove it out." And that's what we did with our original, our pilot concept.

And it did start very limited. We built everything from the policy side of the house, we used NIEM [National Information Exchange Model] to do the data exchanges, we used early versions of GFIPM, and we used the Global Reference Architecture across the board to really prove it out and it worked well.

Di: Mike, do you have anything to add to that? From Nebraska's perspective, what does this information sharing enable you to do that you couldn't do without it?

[00:06:00]

Mike: I think there are two aspects to that: one is the data, which is obviously important. Maury mentioned the depth of data and the detail that isn't necessarily available across state lines, or through NLETS, or things like that. All of the states involved in CONNECT had a good portal, a good access to the data.

But the other aspect is the user base. And traditionally, a lot of things like NLETS or whatever, are restricted to say to law enforcement or to a very defined technical connectivity, or a cost issue can be a barrier. And so we're really trying to reach out and come up with a structure to allow us to use our probation officers, or data that goes far beyond what is available maybe in the mainstream and find a way to share that. It's a real concern in Nebraska because there were a lot more users that don't have NCIC access than do. And so, we wanted to find a way to maybe reach across.

In Wyoming, we've got a shared border. We've got a shared border with Kansas. Parole, probation, that's all a concern to be able to deal with those populations since they are really mobile.

[00:06:59]

Di: Very mobile populations. At this point, I wonder if we could just ask John Ruegg, do you have any other things to add about what you see in terms of the CONNECT Project's business drivers or what kinds of capabilities this enables the participating states to have?

John: Well, I think the CONNECT Project, by adopting the federated identity standards, really accomplished one big goal, which I think is common pretty much with information systems sharing across jurisdictions anywhere in the country. And that is the single sign-on.

We have lots of systems that – whether it's the probation officer, or whether it's the attorneys, or whether it's the law enforcement – in today's world, there's a lot of electronic information that's important to get your job done that does not all reside in your local organization's databases and you need to get access to other people's systems.

[00:08:06]

And typically to do that there's a long process of setting up MOUs. And then I would say typically you get a new user ID and password for every one of those systems. And one of the complaints that we get – and we've been getting for many, many years – is, "I have to remember all these different passwords for all these different systems." So people end up remembering one password and they use them for all systems. And then they've got to update them and refresh them. So it's not a very friendly user experience.

By moving to the federation – where each organization manages its own users, authenticates those users, and vets those users – and then you set up this trust between the systems. Being able to accomplish a single sign-on is really, I think, a big benefit that you can't accomplish without adopting this particular model.

[00:09:01]

So I think that was a big selling point.

And the other thing is that the rules for access to sensitive information from say Alabama to Wyoming may be very different than the rules for access from Alabama to Nebraska for the same types of information, due to differences in state laws.

So the other component of this whole architecture is externalizing the rules and actually having a little rules dictionary about what information you can access and not putting that information buried inside of your application systems. But having that something that the business analysts and the management people can say, "This is our policy for Nebraska. This is our policy [for] users coming from Alabama." I think that's another big benefit.

But essentially, this whole topic today is addressing security across different organizations –

[00:10:01]

– in a way that provides these other benefits like single sign-on and better manageability of the policies over who can access it.

Di: So just to drill down on that for a moment, the benefits from a user's perspective, Mike, help us understand the day in the life of a Nebraska probation officer. Have you achieved single sign-on?

Mike: In Nebraska, as with I think a lot of other states and jurisdictions, we developed a data portal – a criminal justice data portal – that provides access to a wide depth of data: criminal history, probation, jails, corrections. We've partnered with some non-traditional agencies like DMV [Department of Motor Vehicles], Department of Labor, schools – [we're] really able to provide a lot of data at their fingertips. So for probation officers and others, it really is a matter of having one spot to go to, to be able to search data, to be able to access data, and do their job: process probationers, do PSIs [pre-sentence investigations], and things like that.

[00:11:00]

So they've become very focused on having data in one spot and being able to do that. When John mentions single sign-on, we've worked with Wyoming, for instance, and some of our users log

into the Wyoming system, WyCJIS [Wyoming Criminal Justice Information System], with Stephen Myrum out there. Similarly, Wyoming users log into the Nebraska system. And it gets back to that same thing: here we've got two great systems, why can't they talk together?

So by going to CONNECT and by trying to establish those things, we're really breaking that down and getting that granularity of what data people can get to, how they get to it. It used to be really an "all or nothing" kind of thing. And some of the great things about GFIPM and about this technology is you can really tailor it to a state, to a statute, to a user, even, and really make that difference all the way across the board. So I think it's really beneficial, it's going to stretch out how we get at things, and how we're really able to provide data to the users – all the way across the board, whatever they be, probation or others.

John: I think Mike brings up a really good point. In

[00:11:59]

establishing a portal for your internal users – and then behind that portal those resources may be in all of these different states, or localities, or other jurisdictions – but what's going on behind the scenes is when I log into that portal, I have a certain credential and identity and that's being projected and trusted by these different resources out there. So that, when I click on that one item, I don't get prompted for yet another ID and password because now I'm going to Wyoming etcetera.

I've seen portals where they'll set things up, but when you click on it, then you're logging into that particular application. You click on the next one . . . . And so it's important to designate that the portal is not just a front end to a lot of systems that you have to individually log onto. But using this particular framework, the portal lets you go to one place and each of those systems can rely on that one login for getting to those resources.

[00:13:00]

Maury: And time after time it is proven: the significance of single sign-on is so dramatic to being able to have better productivity in your work, to accomplish more, especially for an investigator. There are a bunch of portals out there: whether the federal government provides LEO [Law Enforcement Online], or HSIN [Homeland

Security Information Network], or our state version – AlaCOP [Alabama Communications and Operations Portal] is the name of our portal – or you could continue naming different portals out there. Our folks in Alabama end up using just ours, because they forget, continually. If you haven't used a portal in six weeks, then you've got to go through the process of renewing your password and so forth. And it makes all the difference.

And so our vision – and I think where we're really moving forward on GFIPM – is the possibility [of] ultimately allowing a macro vision of federated identities –

[00:14:00]

– to go out there and allow usage of these other systems the same way we have internally within the state, hitting single sign-on. And it's going to make such a big difference in the long run.

Di: Because all of those transactions that are going on behind the portal now for your users are transparent to them? They don't even need to be concerned about how it's happening; you've just enabled them to reap the benefit of all of these different data stores?

Mike: The word that keeps coming to mind, I have to tell you, is "convergence." As we've gone over the years, the technology has really come together: from the security side, on the database side, on the access side, on the connectivity side. And now we're finally seeing that ramp up a little bit more on the security and the connectivity and everything else. So that the 13 passwords are going into one, in one spot, and it's a great benefit to the user, by all means.

[00:14:57]

John: You know, the ability to do federation – which really means I can use one credential in my local organization and it's honored by these other organizations – that standard did not really come together or get into commercial products until about 2005. And I've been watching something like Directory Services and LDAP [Lightweight Directory Access Protocol] and Active Directory – it's been around well over 10, 15 years. And it takes about 10 years for something to really become mainstream. So finally, I'd say right now, we've moved into the beginnings of mainstream

with federated identity. And we're just starting on the authorization part of the federation.

When you say, "Global Federated Identity and Privilege Management," the privilege management or the authorization piece, we're still really in a very early phase there. But the maturity, the products that are out there in the marketplace for federated identity are pretty much prevalent –

[00:15:59]

– in all of the major vendors' product suites. So there are tools today to make this happen, that really, in 2005, the vendors didn't really have the tools, and so a lot of this stuff was very much "cutting edge."

Mike: That's where the standards help, as well: you can give them to more than one vendor and have everybody working with different products, different vendors, and being able to talk to each other, because of the standards. It's a very good thing.

Di: There's another aspect maybe to the single sign-on – kind of the converse of the ease of use for your user community – and that's the idea that you can more tightly manage the provisioning of users and the ***de***-provisioning of users. Could you talk a little bit about that, Maury? About how you don't have to worry anymore that a Nebraska probation officer has been terminated, but you don't know that, and there's still an ID and a password for your system floating out there.

[00:17:02]

Is that an important business capability for you?

Maury: Oh, absolutely. One of the nice things that was brought to the table by our relatively mature state-based systems at the time is we had a management capability in place. And it's more than just technology now, there's policy behind this, there is legal authority behind this. Much has been thought out about the way we manage users and what their access to data is. And it's very role based, I mean, in terms of what do you have legal authority to get to?

So we take that and when we created CONNECT, we did not work on technology to start with. Right out of the shoot, our very first

activity was dealing with governance and dealing with policy matters and how will we deal with trusting that –

[00:18:01]

– if somebody in Alabama can no longer access data, they can't go through the CONNECT portal to get to Nebraska. And can Mike trust that we can handle doing that? So, yes, we spent a considerable amount of time putting forth some policy direction and guidance to make sure this happens. And then it just flows very well once we have those decisions made, how do we shape the technology to make this work? So the idea that we can now de-provision somebody works fairly seamlessly: if we at the state of Alabama level turn off privileges, then it carries straight through the system.

Di: Mike, do you have anything to add to that? This idea that maintenance of these extensive user tables, and IDs and passwords –

[00:19:00]

– maybe you have a better handle on it?

Mike: Yeah, there might be two aspects to that. One is the underlying ***necessity*** – not just an assumption – that the systems that we're connecting, whether it be CONNECT or whomever, has that capability for that granularity, and the rights, and the de-provisioning, and the monitoring the users in the first place. And that's really key to me trusting Alabama, or Wyoming trusting Kansas. It's really essential to have that capability there and have that commitment to do that.

The other thing, though, with the policy, I think we're still maturing as we look at things go: the policies across states will raise some other questions about what happens with Alabama data that is maybe consumed by a Wyoming user, but misused in Kansas. Who knows? There are still issues with all of this stuff. So even when we talk about the technical aspects or about a lot of the policy issues that we know, and we know we need to deal with –

[00:20:00]

– it's all part of the bigger picture that I think we're still going to be sorting out for awhile. But we have to get there. We have to start, to be able to know what questions we have to ask and how we need to address and deal with them.

Di: Anything to add to that, John?

John: Well, I think it's important to recognize that not everybody out there is supporting a federated model yet for access to their systems. We have a long culture here of every system managing their user base, whether they're from outside the organization or not. And many of them are not in a position: they don't have the foresight to support federation and they're going to continue. So we'll still have multiple IDs for our organizations, but the degree that the trend toward federation grows, then we'll have fewer IDs to de-provision. Now, if everybody was in the federated model –

[00:21:00]

– you're absolutely correct: ***one*** de-provisioning. Since everybody is relying on that one authentication event that says, "Maury Mitchell logged on this morning," as soon as you turn off that local log-on, every other system says, "If you didn't log-on to Maury Mitchell's system this morning, then you're not getting any access." So it really does take a burden, and a quality issue is improved by moving towards federation. So it takes a real burden of de-provisioning off of all the source systems out there that you want to access.

Maury: And let me add, I think the idea is, there is a change of mindset in the way we access data. The traditional silo, we almost overuse that term these days a little bit, but it's true. That's the way it works. There are these silos of information. And it's across the nation, from the smallest micro level of government –

[00:21:59]

– municipalities, and counties, and the state level, and then the federal level, and many agencies. When we started getting into these broader ideas of information sharing, there is a change of mindset. And I think we're seeing great progress across our nation in changing that. But at the same time, now we're facing budget struggles like we've never faced across the nation. There are significant issues that are still putting up roadblocks that we're going to have to overcome. You can't just change your business

operation because you want to. I think there's even a growing desire to move toward trusting more in federated access. But it's easier said than done these days.

[00:22:56]

Di: Mike, would you like to elaborate on that? Has there been a need to educate your user base in Nebraska about what's possible and what some of this technology can gain them?

Mike: Yeah, but I think over time, people will know what's possible just through their day-to-day life.

Di: Like eBay and –

Mike: People are used to eBay and Amazon and being able to go on and Google anybody that they want to, and have all that information come up. So then they turn around and go, "Well, if I can do that with a Google search, why can't I get it on my desktop?" It's an expectation that's there, and I think we need to fit that.

But we need to know the ramifications and knowing that the data you have within your local or maintained criminal justice databases is the real thing, as opposed to maybe some of the things that you're going to find on the [Inter]net. You have to balance that off. So it becomes really tough.

And as Maury mentioned, with the budget cuts, all this is great, but it does cost money and there's stuff on the backend. But that's what the users don't see. They just know that they want to go on, they want to click, and they want to be able to go out to wherever it might happen to be and get the data and bring it back.

[00:24:03]

And they need to do that. There's a real benefit to that and there's a cost savings and a benefit to them being able to do their work better. So it really does extend. At times, it can be tough to kind of quantify that savings or even what that cost is, though. You can talk about a system cost, you can talk about time savings, but it becomes really difficult, because you're changing the entire way that people work.

You talked about the average day. The average day has changed: over the course of the last 10 years, it's changed dramatically. We

see people doing their job differently, working with other people, with other states, differently. And so I think we need to keep all that in mind as we move towards that. It's not just data querying; it's workflow, it's data access, and it's processing things.

Maury: The technology alone, you expect data in different places. I mean, just the incorporation of smartphones now in the daily activity changes so much in the way people work. So we need to take advantage of that. How do we inject the right information –

[00:25:01]

– at the right place, versus just knowing, "Well, I have to go here and get it." No, wherever you are, you should be able to get it now. But that leads to these –

John: This is our consumer market today, and it's important to recognize that where Google and my Smartphone can get is because that information generally is public-record type information or it's a commercial offering to sell you some kind of feature or function. But the data that we work with in the criminal justice agency has, as its basis, restrictions on who can access that information and for what business purpose.

And so we have to introduce some security controls that the Googles and our smartphones they don't care about and they don't need to enforce, because it's not sensitive data that you're going and accessing. And so, a lot of our users are expecting to have these capabilities –

[00:26:00]

– and we're the party of "no." You know, we keep saying, "No, you can't do that." And when they say, "Why?" well, it's because we need a good security model in place and that requires some effort both on the people that are providing the information and the people that are connecting the users to that information, which is basically what we've been talking about today.

So there's work involved and agreements and a lot of things to share criminal justice information that is not the same case with a great deal of the information that's available today on the Net.

Mike: I think sometimes when people look at the complexity of security, they say, "What's the risk? I'm a law enforcement officer. Let's

make it easier for me to get the data. So what if something wrong happens?" But then you open the newspaper and see identity theft and everything else happening and data getting out. You can't really open that door "a little bit," because opening security a little bit is opening it way too far. So it really is a tradeoff.

[00:27:00]

Maury: The domino effect, too, of providing this data so many places and so easily accessible – we have to spend our time as policymakers, as decision-makers, taking care of this data, making sure that we're looking at the citizen's privacy. One thing I've noticed is now that officers have greater access to data, when they also think about the way they do Google or other information access on the internet, there's less of an awareness that, "Wow, this is something sensitive. This is someone's life. This is something I need to be careful about," because it's so easy to get to.

So one nice piece to me about where we're going with this, the technology we're discussing today, is not only is it helping us determine security, but it is also raising an awareness –

[00:28:02]

– of privacy, of responsibility, of holding accountability in there for the users that we couldn't have done before either. So it's the whole package in terms of us thinking through ramifications related to the sensitive data that government provides to ourselves.

[00:28:24]