



## LiveCast 4: July 23, 2020

### Spotlight on Unique Identity Numbers

The following is an **AI generated transcript** of the above mentioned LiveCast episode and therefore may include typographical errors. The purpose of this transcript is to provide quick, searchable reference to the various issues discussed based on keywords you choose to enter.

#### SUMMARY KEYWORDS

system, issued, unique id number, identity, number, unique, data protection, id, data, sector, tokenization, database, national, mauritius, data protection act, card, person, la, country, key

00:08

Within a system so that the same person does not have to re-register every time and that person can continuously be identified uniquely for that, within that system. And in the case of the financial sector, this is very important for the integrity of the financial system that it's the same person that is continuing to come back and back to access services. And therefore, it's very powerful for facilitating financial inclusion, then when the same number is used across different systems, that allows data on the same person to be to be matched. So we're seeing this a lot within the context of COVID-19, where countries have had to deploy their social assistance very quickly. And as part of that they've had to check the eligibility of someone, are they registered in a social security program? They do they own land, are they already receiving benefits from the farmers subsidy program, for example. Now, the use of a unique number in some of these contexts has shown to help streamline that process, and to automate it to a great extent. Now, because of the universality unique ID numbers issued by foundational ID systems, like a civil registry, or a national ID, and let's call it a national ID number, or ni n allows these benefits to be realized across many services and programs and potentially all of them. So this is extremely important for the administration of a country the delivery of services, and in many respects, allowing people to exercise their rights and access their entitlements. However, there are risks of a pervasive or a ubiquitous, unique ID number that is exposed and used. So first of all, in terms of privacy, and it allows the unlawful or unauthorized or unwarranted correlation of data across systems. And this can lead to surveillance, and it can lead to far worse consequences because the use of a unique ID number across systems also allows that to be used for good and for bad purposes. And then in terms of security. If the if a unique ID number is used for many purposes, and it's used as part of verifying identity, then, if it's ever exposed or breached or lost control of then that person's identity can be assumed, right. Even if there is a strong authenticators, such as biometrics, there is still a risk of relying

parties who use ID systems. So for example, banks or credit card companies or government agencies, they still often just use a unique number. And therefore it doesn't necessarily completely safeguard against such risks. Now, these risks become greater when, when the ID number is permanent, as what a national ID number usually is, and when it has more users as what a national ID number normally does. And these risks are present across four areas, at least four areas. One is when they're printed on an ID card. In many countries, it's commonplace to hand in your ID card, when you when you enter a building, right? And and that ID card can be photocopied, scanned, etc. And so then you lose control of it forever. And also, when you're filling out forms or in the middle of transactions, when data is going, for example, from a point of authentication to the system that authenticate somebody, it can be intercepted. And finally, and and and what we've seen a lot of is when the ID number is seeded into many databases. Now on that issue, and often when and when an ID numbers are seeded, and there is a breach, it's actually often not a breach of the ID system itself.

04:05

In fact, in many cases is beyond the control of the ID system. But the public perception may be different. The public will say the National ID numbers were breached. So the National ID system was breached. And so this is not just an ID issue. In fact, in many countries, you've got four examples here in South Africa. 60 million national ID numbers were leaked from a real estate database. In South Korea, a credit card database like many million in the US, the famous Equifax breach. It's a credit bureau that they it wasn't a breach of the social security card system. It was a breach of Equifax. And then in India, there's been many allegations of the Aadhaar being hacked, but in most cases, it's actually that that the relying parties who store that number are being the ones that have been breached. So once once an ID number is generated, or once an ID card is personalized, the ID system often loses control over it. So it's very crucial that Id agencies and and governments as a whole, including the data protection authorities, and other regulators think of this in a holistic manner.

05:12

How can they? Yeah?

05:16

Sorry, slow down,

05:18

slow down to speech.

05:19

Okay. Okay. So how, how can the risks be mitigated. So there's two activities that are absolutely required. First of all, is having legal and institutional safeguards that govern and enforce how, and why and when national ID numbers or other unique ID numbers are used. Some countries don't allow the private sector to use it, for example, the Netherlands, some countries have very strict restrictions, even on what government agencies can use national ID numbers such as Singapore, and even New Zealand has completely banned unique ID numbers that are used for multiple purposes. But then there's other that, you know, there's other degrees of how this is governed. But what's very important is that there is accountability and oversight over this, and rules about what happens when something goes wrong. And

then there's strong information and cyber security. And that involves protecting the systems, the networks, things like masking encryption, identity and access management, etc. For the systems and networks that actually use and consume the National ID numbers and other UI ends. But it's very important to note that no security measures are going to be perfect, there's always going to be risks and vulnerabilities in the system. And there's always going to be bad actors who with enough resources can do bad things. Now, some other strategies that countries are adopting. Here's three examples. This is not exhaustive. But the first one is tokenization, which I'm going to talk about in a little while. And tokenization, as it says there is about not preventing the use of the National ID number, but hiding it or protecting it, because it's a sensitive piece of personal information. So it can be hidden through various means. And while it's being used or stored in the ways in the four ways that I mentioned earlier, then their sectoral ID numbers. So countries made to find sectors like the health sector, or the social sector, the financial sector, who would share a unique ID number, and ideally that those would be routed on a national identity. And then there is another layer, which is the authentication layer and Federation or decentralization of the credentials that facilitate that, that authentication. So this distribution of the the functioning of the open ID system reduces the way it distributes the transactional data. So So that sort of mitigates the risks or distributes the risk. Coming back to tokenization. And I want to talk in a bit more detail about this, because perhaps of all the strategies, it's the less the least intuitive. And bear with me, it's a complex topic, and it's not easy to explain this on a single slide. Now what it is, is substituting a sensitive piece of data or an attribute, such as a national ID number, with a non sensitive equivalent, and that non sensitive equivalent actually has no value by itself. But it can be linked back to the sensitive information through what's called a tokenization system. So the tokenization system may do this the linking between a token and its route with cryptography or an algorithm or a map. The Austria uses cryptography. India through adhaar uses an algorithm and perhaps other countries could use a mapper which which is not a sophisticated technology, but stick but but perhaps easier to deploy. Now, what's very important is that tokenization system or a good one, can facilitate the matching across systems that I mentioned earlier, which is a key benefit of unique ID numbers. And and what can also happen as part of that tokenization system is that it can govern the rules that allow various parties to match that data. So for example, it might require the consent of the individual, or, or and as well as the legal basis. Now what's also important about tokenization is although it may be a new topic for the identity, a sphere, it's actually been used for decades in the payments and credit cards industries so that the the technology itself is mature, but maybe not so much within the context. Have ID systems. But nonetheless, generally, it's mature. As I mentioned earlier, several countries are already using it, I refer to Austria, who have a very unique and sophisticated system with private keys stored on the smart card chip, you have France who uses it as part of France Connect. And then you have India, which I mentioned earlier as part of Aadhaar. And in Nigeria, we're very excited, he's going to be deploying it. And we look forward to supporting them as part of that journey through through our ID for the project that and and it's it's good to note that tokenization is part of the modular open source identity platform or motion, and which is an open source freely available ident core identity software that any country can use, even if you don't actually adopted, you can look at the code, scrutinize the code, and study the design for how each country may want to implement it. So there's two kinds of tokenization, as you can see here on the right, that are facilitated through that tokenization system. First is front end tokenization. And this, this is when a person that Id holder generates the token for themselves. This may be for a particular time period, like six months, or one month or a day, or for a particular transaction. And it would be used in the same way as a national ID number. And the example is the

Aadhaar virtual ID in India. And then there's another, you know, more simpler version of that, which is, I mentioned the the permanent ID number being printed on the card. But what what if you printed a token that was only valid for the value for the life of the card. So for example, in the Philippines, they're not printing the fiercest number on the ID cards, they're printing a temporary filss card number, there'll be a new one will be generated each time a person gets a new card. Now, what's also important about front end tokenization is that this requires acceptance by by people by the public, the citizens and the residents, and also the relying parties. So it can be complex to implement. Then there's backend tokenization. What happens here is proceeding after successful authentication, the tokenization system would generate a token that would allow the relying party to store now in the case, I mentioned Austria earlier, it's called the SSP. And this requires only acceptance by the relying party. So the citizens or the people don't have to do anything. So it's probably easier to from one perspective to deploy, because you don't have to educate, you know, perhaps millions and 10s of millions of people. But relying parties need to be able to adopt that system. And so for example, in with Aadhaar, I think it's a 56 alphanumeric token that is generated. So

12:51

state government, aka social protection agency needs to know that they're not going to get the 12 digit Aadhaar number, they're going to get a 56 digit alphanumeric string.

13:03

So I'm going to conclude? Yep. Yep,

13:06

I'm going to conclude my presentation just with these key messages. So the first one is that the UI ends must be protected to mitigate those privacy and security risks that I mentioned. But also they must be protected in such a way that doesn't prevent the lawful matching and, and unique identification that I mentioned earlier. And this is not an ID issue. It's actually a whole of country issue and a whole of society issues. So it needs to be looked at through a comprehensive holistic lens, strong legal and institutional safeguards and and cybersecurity Information Security postures are essential. And the benefits that I've described can be realized through some of these strategies that I mentioned, such as tokenisation sectoral your unique ID numbers, and alternative authentication methods such as decentralized or federated models. And importantly, these are becoming more accessible and more realistic. But But the big, but the right mitigation strategy for each country will depend on the local context. And that includes the maturity of the ID system, the maturity of the legal framework, and the willingness of relying parties, the ID agency to to implement such measures. Thank you very much.

14:26

Jonathan, thank you, thank you very much for a wonderful presentation that really highlights the richness of this subject and the challenges that we as the identity community working together would need to overcome to produce the right identifiers that respect privacy, but enable still the linkage with services across government sectors. Um, Before we continue, and women are going to debate sessions, but I want to do a quick poll. So I defer Africa, moderator can Please run the poll. And please, attendees respond to the poll. It basically says just a very simple poll, what do you think the identity unique ID number? Should it should be the same number used across all sectors? Or should it be

different for each sector, the rate at which Aquila memmio truly sector, the outward digital shock sector. So just just a simple attitude Reality Check that we want to start with. So we'll see 42% have voted will give you more chance to vote. So please give us your opinion, we want to hear about that.

15:45

Clearly,

15:47

it's not a scientific poll, but at least it gives an indication for where the attendees and the community mind is the second segment of this session. But today, we are going to go country by country and ask the panelists to give us their perspective about the subject. What do they think if the country has a unique ID project identity project in place? What is the structure of that unique ID? And how are they protecting or not protecting? If the issue of privacy maybe is not a serious issue in the country. So I'd like to in fact, we have 64% of the vote, I think I will stop the voting here. As you can see, 66% have said unique universal and 35% believe it should be different for each sector. So we're talking about two thirds one way and one third, the other. Okay, so let's keep this as a data point, as we continue the dialogue. My next guest, Jonathan, thank you, but I'd like you to stay because there will be questions that you may want to help us with and participate with your expertise. Thank you so much. My next guest My next guest is Omar Seghrouchni. I will address Omar in French

{French transcription not available}

....

23:25

Okay. Okay, a lot of opportunity to debate and discussion. I will continue now by asking the perspective of Nigeria. We understood Morocco, there are some reserves from the Data Protection Authority. However, you believe there is potential for resolving the issues by adopting some tokenization technologies as explained by World Bank, Jonathan. So let's move on and ask the perspective from a deja vu can take no more than four minutes so we can give the debate some dynamic.

24:07

Very much. Good day everyone. In Nigeria, what we have done was to get the policy directory first. As you all know, we have gone through the identity system before which was data collected and cards issued. So the policy directive this time around was to have an identity management system and identity management system that was built on privacy for me from the initial stage. So it's a system privacy design system. So what we do is from the point of data collection, to storage, transmission, and then to access to that database, the issue of privacy was considered from the equipment It has the whole technology, the network infrastructure, and even with respect to the human resources, because each and every staff or consultant working within the Commission has to go through some security, screening and things like that. So that's what it is that the national identity management the mandate given to the national identity was established under the Act of 2007. So there was a parliamentary legislation before the thing started. And the mandate given to the commission is to create manage operator initial identities, and the system, the whole system from the what we call the front end, and the

back end, middleware and network infrastructure are all part of what that means he needs to create, protect or regulate. So where we are now is we have build the infrastructure, both front end and back end, the front end, which consists of a ruler system may not have been adequate as we are. But when going into the ecosystem, the partnership we are having with the World Bank, is to make sure that that section of the project, the infrastructure is the data population is enhanced, and we have wider coverage across the Federation. And then the backend also, we have a robust back end system, we have a primary database, and then a secondary database, which is about more than 200 kilometers away from the primary data. And the middle where because the way that the infrastructure was was done is not to have a single vendor controlling the whole back end. So we have a fragmented system whereby we have we have a middleware that interconnect the different parts of the backend. So the database, the secondary database, and then the PCI infrastructure, and also the the payload card, personalization are all part of the backend, then the network infrastructure to ensure security, we made sure that the Metropolitan Area Network we have in Abuja connects to 14 government agencies, all these 14 agencies are part of the equal ecosystem that collects data for the respective functional requirements. So they are connected to the national identity database to the fiber optic network. And then our state offices in 37 states including Abuja also are connected by to fiber and then the larger enrollment centers in over 900 locations connected by besides internet dongles from the network operators. So the system is we have we have taken the pains from the initial stage of the design of the national identity management system to incorporate issues of privacy security, but as a nation, we know there is the challenge of data protection, a national data protection law tree, but that's with by the end of this 2020. These are the work is already in progress in earnest to make sure that data protection, lowering is this by the end of the year.

28:52

Okay, Hadiza, sorry to cut you, but I want to keep the dialogue going. I want to ask you a question. You have said that there will be a unique ID number name, will that need to be used across all government services? So it's a unique number, not sectoral number?

29:11

Is it? Do we have a unique number however, the different sector shows the different other agencies that is that collect data issue, there are no sectorial IDs. Like for the bank, we have what they call the bank verification number, there is a driver's license. This is a passport for the individual passport number for the immigration. But then the important thing is the government policy is that all those other government databases that capture data and issue their sectorial, who functional IDs must be linked to the unique national identification number,

29:49

but there is no requirement that the union be publicly used. In service delivery, you give it it says in the behind a back end and then you can use the sectorial number, for example, the dvn, you see the bvn in Nigeria dying, or do you see it continuing to be used?

30:08

No, it may continue to be used by the bands. But the way the way we do it now, because most of these agencies have access to the National ID database, or the harmonization, we have done with the, with

the BB, and we harmonize the APB and data with the National ID and we give them back the national identification number. But we have we have had a rethink of that, looking at the larger security issues and like General, Jonathan stated in his presentation tokenization. And hashing is another model that we are using for subsequent harmonization that we are going to embark on, even for access to the national identity database. Because right now, the verification access from both public and private sector agencies, they are able to see the need. But going forward, which we will, we have reached an advanced stage in our development, and our product. So going forward by all of us as well, we want to launch it by the next September 16. To launch that product to make sure that we forward the rights to present an ID, who will be in the hands of the identity holder through tokenization, you have a token you give a token and that token can only be utilized or utilized by is one single service provider that you presented it to, and it will have a lifetime, a lifetime of 30 days or more, depending on the threshold we want to send you set for it.

31:46

Okay, that's actually great news. Because what you're talking about not as the old concept of 10 years ago, when you had a centralized database, with everybody in a single number, everybody is issued a unique number. And then it's linked. services are linked. So we're talking about the future of unique ID, which seems to be a form of tokenization, or allowing control in the hands of the owners of the identity, working with the sector themselves. So additional giving us wonderful news. So you've heard it here first. So let's continue with our discussion moving forward. I think before I do that, I want to I want to take a point and answer a question. Somebody asked anonymously, that, in our previous session, they said you want to move the objective of identity for all from 2030? I think it's Robert Palacios, who said that, that to 2022. And today we've heard from Jonathan, we've heard from many others who said the legal framework is very, very important. And do we think we're going to be ready to have legal frameworks in place by 2022. So that we can actually achieve this objective or this was just a moment of enthusiasm. That is not 100% realistic? Maybe I can I can I can ask one of the panelists if you have any. Any comment on that? I mean, are you ready? Are you ready with the legal frameworks to allow to the acceleration of 16.9 by eight years?

33:29

Ah,

33:30

I believe Nigeria is very ready. We already have the legal framework for the identity sector, we have had policy decisions on the ecosystem. We have cybercrime, prohibited and provision act in place which is undergoing a second review. And the data protection bill should be running by the end of 2020. So for Nigeria, I think we have prepared ourselves because our ecosystem will not move forward if we don't have those legal instruments.

34:04

Okay, so for all the other panelists, when it is your turn, please address that issue. Whether you think your country will be ready. I want to continue, actually, since Drudeisha Madhub has joined us earlier than expected. delish. Are you ready to give your prepared remarks?

34:42

Okay. So the question is, we would like to hear the perspective of Mauritius about where do you stand on the money can you believe it shouldn't be a one universal number. Do you think it should be multiple numbers link? Do you think you want to do that? organization. So give us a perspective from Mauritius.

35:04

Okay. Thank you so much as if yes, I guess all the issues about what is the importance of having a unique ID number has already been put on table. What I'm going to focus on is actually Mauritius has been ready since 2013. With a unique I must say the unique ID number was here since a very long time ago. But the way the new smart ID card has been introduced, it's only in 2013, that actually, we had a new smart ID card. But the concept of unique identifier, has existed a very, very long time ago in Mauritius, with the enactment of the National Identity Card, I'm talking about, let's say 50 years ago, so that concept was already in place in Mauritius. But we came forward with a digital unique identifiers since 2013. And they are novelty in that new identity card is that once a person is issued, with it's a national, unique ID card, actually old information that is stored on that ID card, for example, His fingerprint, or any other biometric information that the card or the chip may contain actually belongs to the owner. Only that is only the individual has the possession of that information, which is on the chip, or the card. And no other body has this access to this type of information, except that the national identity card or agency, once it is issuing the card, it was still the fingerprint data for a minimum period of one day up to a maximum period of seven days after that, it will be erased automatically, and the government agency won't have access to this information because it's no longer in the National ID database. This was in consequence to private counsel judgment, after long battles in court as to why fingerprint data or any other biometric data relating to data protection issues, obviously, has to be stored on the national identity card. And it was a basic, I mean, a wonderful victory for the data protection. perspective, because we actually erased that fingerprint data from the chip.

37:39

I mean, storing there is no such issue as storing, but the data is on the cop, whereas so tokenization is already in place here. And if I can use another word for I mean, moving forward with tokenization is actually what we're talking about is anonymization as well in data protection, jargon anonymization is very important is that the concept of giving a number to an individual actually, you are protecting his personal data from public viewing, or, and that is a very basic principle in data protection is that we need to anonymize data as far as we can to protect an individual. And tokenization is actually one of the ways of achieving anonymization, which is very much appreciated in our in our data protection law. So we already have this legal framework in place. And there is no problem actually, that we have encountered. Actually, we, as the Data Protection Agency in Mauritius had the opportunity of auditing, of checking how the information has been deleted, if it's truly being deleted, it's not being stored for or you know, to get on the fries access to this type of data. And we were satisfied that things were going in the right direction. So this is one basic point that is very important for me to highlight. And in our legal National Identity Card act, we actually have a provision specifically saying that this collection of data should be in compliance with the Data Protection Act of Mauritius. So all the principles that we have in the Data Protection Act actually being applied to the unique identifier, a way of handling data. So I think from that perspective, we should be quite happy on our side that we are actually implementing data



protection from a very efficient in an efficient way. And as I must say that our privacy by design has been incorporated in that chip. So that The information is actually very secure. And there is no way that someone can access this without the consent of the individual. So I would stop here, if that answered the question that you put to me. Yes, thank you.

40:16

That answers the question very well, if I were to summarize what you said, I mean, Mauritius has a unique ID number, but you are not concerned as the Commissioner of the Data Protection Authority. Because you've implemented strong data protection measures that go along with that unique ID number, it's not a unique ID number in the wild, you are able to delete data, you are able to restrict access to data. And that's why in your case, tokenization is not necessary.

40:49

I don't mean that tokenization is not necessary. But we have gone much forward with with I mean, the very fact that we have a unique ID number, which does not depict the personal information, or the person who's actually we're going much further than tokenization is required. This is what I meant to say. Okay.

41:13

Okay, somebody is asking a question specifically to you. I'm not sure I can understand it. But let me read it. How do you prevent fraudulent cards, which replicates the format of a true identity card containing biometrics? I assume the cards are issued on the cryptography keys? No,

41:30

exactly. The problem here is that big being given that the ownership or the card is that of the individual that is it's his card, it's his identity, it's his number. So if there's any kind of illegal activity that is being done, obviously, there is a legal framework for that. We have what we call the Computer Misuse and cybercrime act, in accordance with the Budapest Council of Europe convention, which follows all the principles to protect the information and the cyber cybersecurity risks that may stem from any fraudulent activity being done with the court. So we have this legal framework. And then we have other institutions in versus what we call the cert, which actually handle a computer incidents. And we have a cyber crime police unit, which also handles cyber crime offences being committed. So these are the agencies which look after any type of fraudulent activity being done with any card, any misuse of any card. And we have a very, I must say we have many cases in commercials which have been reported and successfully completed by the police cybercrime, the cert and the data protection office to some extent, because we also handle personal information. We have had cases as well, relating to personal data being fraudulent to us that were reported to the data protection office, I must say also, we handle these inquiries quite well. And the outcome has been successful. And because also any type of infringement, or the Data Protection Act is an offence is a criminal offence under our law. So we prosecute people, even under the Data Protection Act, we don't really need always to go under Computer Misuse, or any other electronic transactions act, for example, we can also use the Data Protection Act. And this is like the panoply of League legal legislations MSA legislations that we have, which go in the same direction. That is criminal sanctioning.

43:37

Okay, thank you. Thank you so much. You've got legal frameworks, you've got criminal institutions that look after the abuse and then you also have technical measures in place so unique ID number can live without any concerns to the data protection authorities problem.

{French presentation follows on Gabon – not transcribed}

52:51

Okay, there may be this perspective of a unique identifier in Africa, I would like to give a little bit of a background in the Kenyan context, in terms of having a unique identifier number. And also using identity can't let God have a unique identifier. First of all, in Kenya, at the age of 18, everybody's issued with an edited account, which is unique and is unique because it's tied to his biometrics to the fingerprints. That number which you issued at the age of 18 is the number which is now used by all other organizations, for purposes of issuance of wellness services. Either one is trying to apply for a driver's license. First of all, you'd have to authenticate the identity card number, not an ad, then the card number in the database, so that you are sure that the person whom you're issuing will, the driving license is the same person who is holding that ID and the same cut the clothes or other services. It's with our tax system, how I held the system on such a current system, you require your identity card number, which is tied to your biometrics and of course, now the ID in terms of

54:23

how effective it has been. Our goal may be to all aspects of the Kenyan, public even electoral system, you cannot register as a voter, if you have not been issued an ID, and it is the ID which is used by the Electoral Commission for purposes of registering an individual as an elector. Actually, by law. If you cannot vote when you don't have an ID, and all aspects, whether it's in social banks. You cannot open a bank account, if you don't have an ID and the bank's cross reference with the database, for purpose of indicating that the person who is opening the account or person who is carrying the transaction is the person that you pass on the holder. So for this discussion, maybe it's rook is important to cut it in the two segments that first of all, the Identity Card must be tied to the biometrics or any other reference, again, the identity layer, the identity of the person who is this a unique identity, identity would have to now get an ID to authenticate the particulars of that individual. Kenya 95% of the population have an ID and unique to them, because you reference them on the biometrics, the biometrics, I hear that at the National registration bureau database. As of now, we don't have an electronic ID, that's what we are, we are trying to develop one right now. But we don't have one. But even in terms of the cotton candy, which isn't that no, it's not electronic, you have a fingerprint. And we have fingerprint tells us all over the country, the police, they are trained for purpose of identification of a of the some, some of the policemen are trained, so that in case somebody presents an ID, and you want to be sure that it is the case, in person, you have a law, you'd have to make use of the naturalization bureau or those trained policemen who will know about the fingerprints. So you tie the identity of this person to his biometrics, and as I said 95% of the people above 18 have a unique identifier, our work you must be those below 18 that is a those who may not like your job minority, because you buy those I should buy certificates. But even for that, let me make a clarification even for those below 18 you cannot be issued, you will buy certificate if the identity card of your parents is not indicated in the university. So in terms of the

indication that the child you are issuing a birth certificate with is the child of a Kenyan, you'd have to rely on the unique identity card number of the parents. So that has been our missing a missing segment in terms of having a unique identifier for the whole population. And that's why we have embarked on this national integrated system which a lot of you have heard called the huduma. Where we want to start issuing a unique advantage and find out about a child is born is issued with a unique identification number. By the time that child is going to school primary school, our plan is to start capturing the fingerprints so that fingerprints would go to the database at the age of 18. It is under for that job to apply for an ID Andrew issued it on the spot without necessarily subjecting that individual to further scrutiny.

58:31

Sorry to cut you off, we're running out of time so I assume you are on the pathway to issued unique identifiers to the entire population. The adults already have it. The children are getting derived from their parents but you will be issuing them at birth and identifier and that will follow them throughout life. So sorry about that because we're running out of time. And I need I need to hear from Sofiene before we can continue with the community voices. We'll bring you back in Sorry about that. Thank you for that. Sofiene?

{Sofiene speaks in French. Not transcribed}

1:05:40

Okay, Sofia, merci beaucoup. Perfect. I want to summarize a little bit what you said but in English, because I'm not sure that the interpreters were able to catch you Tunis, Tunisia has put in place a very pragmatic approach towards the question of the unique identifier. And the pragmatic approach was not to simply ignore the, the sectorial numbers, each sector has their own number, they think there could be in the long term unique number that can be attributed. But in the meantime, there is a table of correspondence, which includes the social identity number, the national identity numbers, colorization, number, tax ID number, which basically refer these numbers to a unique ID number, which could be attributed. you've implemented mechanisms and measures that allow the owner of this number to know if somebody access the data, I assume this is from a an accessible website or something that is on a mobile application so that they are notified when there is a use of that number. And they could inquire about that. This is a very recent development, this came out in May. So congratulations on that. Clearly, we're hearing an approach that is complementary to the other approaches that we've heard about. I'm going to come back to the panel with some some other thoughts, which I'll ask them to prepare. But in the meantime, sort of think about what closing messages and sort of take home you want one message to give the attendees with. But in the meantime, I want to hear from the community and please the community, there's been six or seven that raised their hands. I want to recognize a few. But please do not take more than two minutes, I will be obligated to cut you off for two minutes. Okay, so please, the first one that I want to bring on, it's going to be Pam Dixon. Could you please promote them to a panel of operators, can you please promote them to the panel? Welcome, Pam.

1:07:56

Hi, am I here yet? Oh, I am here. Yes. So thank you, Joseph. And thank you for a wonderful panel to all of the panelists. It's a pleasure to be here and an honor. Your your panels been excellent. So I just wanted to add on to some of the items that have been said in regards to identity and privacy. I wanted to talk just briefly about a different aspect of identity, which is sustainability. This isn't often discussed in the context of IDs, whether they be federated or etc. But really, we now have a very large body of work, which indicates that in order for ID systems to have genuine sustainability, they will have certain characteristics. One of these is legislative sustainability. So for example, we have 143 jurisdictions now in the world that have passed GDPR legislation, or GDPR, like legislation that is interoperable. And I think that going forward, that identity systems will need to find interoperability at this level, which will bring it more to Commissioner mudrooms level where you have a very strong protection system for the identity number or system. And then I wanted to also discuss very briefly the idea of technological sustainability. So we talk a lot about SDG nine, but there are other targets, nine dot one nine dot four, nine dot five, to really upgrade technological capacity. And really the upgraded technological capacity today, based on our scientific and technological evidence is to have much more of a federated system, or tokenization, or as Commissioner Madhub said go beyond tokenization. So the well the centralized numbers are easier at the beginning. There's a very, very high cost In terms of sustainability analysis over the long run, so I do think that's an important consideration in an analysis of a system. And then finally, I want to talk about social sustainability, which is the role of trust in identity systems. I think we all know and have seen in history, that in order to have sustainable systems of data, we have to have both governments that trust the data, in terms of accuracy, but we also have to have people and data protection authorities that trust the system to be transparent and accountable. So in doing a system analysis, we've got to consider all of these things. Thank you so much, Joseph.

1:10:41

Thank you, Pam. Okay. I will, I will do back to the panel now. And then I will bring back another person from the audience. But I'll go back to the panel. And I will ask, basically, starting with Hadiza, I would ask, what one thing from your experiences. Would you recommend the attendee pay attention to when building a unique ID number of the population? Just one thing? I'm told there are many but one important thing is you're on mute, please.

1:11:19

Yes. The one thing I think every government should take into consideration is getting the regulatory framework, right. Okay. And one thing once you get the legal regulatory framework, right, then it's take care of the technology the human aspect of it and things like that.

1:11:43

Okay. Thank you so much, Omar?

{Omar speaking in French – not transcribed}

1:13:51

Just to tell the audience, the audience, we will be bringing back the subject in more technical detail and in more regulatory detail by focusing on one country at a time within the within the framework of the

CPR, which is the country progress reports, I promise you, we will address this subject. There's a lot of interest. I want to continue with my job. Please give us your perspective.

1:14:20

Yes, thank you, Joseph, I, I believe there should be only one and only a prime consideration to the human right to identity. And that is the protection of the individuals interests. This is my only way to summarize what we're aiming at is protecting the individual. And that is what we should all have in mind including from an international regional or local perspective.

1:14:49

Is this a form of do no harm kind of principle that you have subscribed to?

1:14:54

Absolutely do no harm is just one component of what I'm talking about. I believe we should be always proactive and prepared to really innovate. I believe in every sense of the word innovation is linked to this unique ID card, the way we actually want to do it, in any context is linked to the level of innovation that the country has the level of infrastructure that the country has. But with whatever infrastructure The country has, basically, we can always protect individuals in our own ways. So this is what I believe we should, we should aim. And that should be the only aim behind having whether you sectorial a unique ID number, or even as many tokenization or numbers as you wish. But the only consideration should be it is a human right. And we should protect the individual. Thank you so much.

1:15:52

Excellent, excellent. Okay. Operator, please promote Anita just to join the community in any way, please do minutes or cut you off. Please, Anita from the World Bank, join, join the discussion. And then I'll come back to the panel.

1:16:10

Thank you, Joseph, and ID4Africa for giving me this opportunity. I'm reminded of an image in India when I visited a school, they had a very strong Iron Dome. And what do you see there are no boundary walls. So the middle to protect the UI and by tokenization, of protecting the UI n. But if the security of the system is not in place, we could use other identity attributes, or mobile number to do data correlation or surveillance. On the same note, we know that countries in the EU have built strong walls and doors and use a single identification number to provide services proactively to the users by using joined up services. However, they feel Yes, tokenization may answer the problem of making it difficult to link data. But I would probably like to raise two open questions, which are raised because of tokenization. So as Jonathan said, there are two main purposes, or functions of ID system. One is continuous authentication. So in the context of Africa, if there is no internet connectivity, and the person comes with their virtual ID, or the ID number to identify, how can you link that person's data with the backend token, with the tokenization in place, it's not possible to link with the token. second problem is the act of linking data across databases. So India has implemented tokenization. But we still don't have a solution, which enables sharing of data with tokenization. In the context of India, they have used, they have allowed trusted authorized entities to store the ID number. So I think could design an

implementation of a tokenization system, which allows linking of data with the need of the law. Thank you.

1:18:22

Okay, thank you so much. Yeah, absolutely. We need to be sensitive to the context of Africa. tokenisation might be a complex process, infrastructure, if that does not exist. We have to be looking at other alternatives to protect the interests of the owners of that data. And but always, always within the context of Africa. I want to continue, Ruben give us a closing thought on the subject. What do you want people to remember? From what you said? unmute please. Robin. Okay, we lost a little bit so let's continue with Mr. Massamba.

{Continues with Mr. Massamba in French – not transcribed}

1:21:27

Okay. On pragmatism. Okay, well, good afternoon. But can you put that back in? You have your microphone on? Reuben? Yes. Okay. Sorry

1:21:42

about my system. I think my contribution to this is on three fronts. One of them in terms of the legal framework, our registration of Persons Act protects data, which is captured by the National Bureau for being issued to another individual without the Express ability of that individual. So you cannot access data from other systems and the rest not individual himself expressly, as given for it except for production and other purposes. In terms of the national integrated management system we have coming up with, we have one of the conditions was for us to come up with a Data Protection Act, which was enacted in December, we have a Data Protection Act. But beside that you find there because of a privacy issues a lot of individuals have gone to court asking that there are a lot of safeguards should be put, before we can capture all the data, what you're trying to come up with is to degrade all that data which is held by other agencies into one framework. As we are now you find other agencies use data from the National Bureau, through a system we call the E government where for purpose of a services you rajee in and you're able to process your documentation from one center, but you're trying to come up with a system whereby you have a database where it is all the services you have instead of you now going to various agencies, so that before you process services for an individual, you can do it from one spot. That's what we are trying to come up with. He has his own challenges. Like I said, we have very good challenges. We Okay, technological issues to do with it because it's a new phenomena. As you can see, I say do we already have an a unique number for people above 18 below 18, we have come up with an ambitious program in Kenya to capture the bus or the digitize them. So that the number which will be issued by several industries at the birth is the number which will become the unique identifier for that individual. Okay. Maybe guess my main point of that day, I would say there the use of unique identifier for purpose of a person's country's segment. There is one crucial area security we've created now we have global issues of security, or maybe that's missing by the world. And the unique identity number we have in Kenya is playing a big role in terms of safeguarding us against terrorism and other issues of it of insecurity because

1:24:44

So you see, you see the unique ID number playing a role in the national security of the country. Okay, let's so let's move on, Sofiene. Then I'm going to ask Jonathan and then there will be one more person and then stay tuned because we are going to repeat the poll because I want to see if there's been any change we know exactly the numbers before we run it again see if there's any change in mind or whether you're all in the same point Sofiene please.

{Sofiene continues in French – not transcribed}

1:26:08

perfect Singapore. I want to promote one additional person from the method Professor Henni from Algeria so we got an easy web maroc Can you please promote him to the panel and Professor Henni. And then we'll close with the keynote speaker Jonathan.

{Mr. Henni continues in French – not transcribed}

1:29:36

Okay, excellent. Merci beaucoup. Now, I would like to ask our keynote speaker Jonathan to give us a closing wisdom. And then I'd like to run the poll again. So please stay with us because it's very important to see if there's any changes in the perspective. Jonathan, please.

1:29:55

Thank you very much, Joseph and greetings from tomorrow to everyone from Australia. It's now the 24th. It's been a fantastic discussion, I'd like to thank all the fellow speakers. And I've learned a lot and and the discussion in the chat box as well has been very dynamic. And I presented five key messages in my keynote. And those I believe, is still valid. And I agree with everything that the fellow panelists said in their closing remarks. I particularly want to acknowledge what my dog said about about putting the interests of the people and protecting their interests first or do no harm. In terms of closing thought, I have three for three things that that three tools that I hope you can all use, because it is possible to protect people's identity, and to have the benefits of uniqueness and data matching. Right, it's possible to do those two things. So first of all, is threat modeling. Right? When you're making your decision, and identify and analyze the threats. The second is privacy or data protection impact assessments. Third is work with academics and civil society in your countries, because they probably have done a lot of thinking and examination of the options. And certainly for the wall bank, we've really looked forward to working with, with Nigeria with Tunisia, we've kept on with Morocco, on their journeys, and and many other countries where we work. So please also visit our website to have a look at some of our materials. Thank you, everyone, and have a lovely day.

1:31:36

Thank you, operator run that form, please, before before you go, and before we close, could you please run the poll. And please participate all the Okay, please vote. So we can see where the results are. And, of course, I'd like to thank this while we go composing the the numbers, I'd like to thank the participants, the panelists for a wonderful, wonderful contribution. I think, as always the case the issues

are very, very interesting and rich. So I think they will fuel the kind of discussions that is action oriented that we are going to have to have when we come back in the new season after the break. So please stay with us. In the meantime, do not. If you have missed any of our our series, our episodes, please go to the YouTube channel and subscribe and activate the bell. I think it's very important that as a community, we stay together. So please come back in. Okay. So now we go back. And wait, one more minute, I think of you. We have 58% of the of the vote. And it looks like I just want to wait till 60% of the vote. So at least if there is anybody wanting to vote, we're at 59% voted. Okay, let's not at 60%. Now, please stop the vote and show the results. Okay, so basically, what we're hearing is that 71% should be and should be the same number 320 9%. Believe should be sectorial. In fact, I don't know if it's statistically significant. But I think it seems to have moved in the direction of believing that it one unique number universal. However, I believe because people heard a lot of a lot of good practices to tribute or to add to from a data protection that gives them perhaps the comfort that universal number can work. It's simple, but needs to be accompanied by very, very strong data protection measures. Tunisia has been doing something in that regard. Mauritius has examples also to share in that regard, in Nigeria with the tokenization work that they will be starting to do. So the rich set of experiences that we can look forward to as we move this discussion forward. Again, thank you all very much for your attendance. And please join me in thanking the panel for their time and energy and I apologize for the delay in the session. Thank you very much. See you in September September 3. And my apologies for we've had a lot of people that raise their hands. It's just we didn't have enough time to to allow everybody to speak and participate. It's a good problem to have, but we will be managing it better. So trust me Come back we will have chances for you to participate and hear your voices. This time was a was a first experience for us where we are promoting people to the panel so they can raise issues and get off the panel. impromptu. So thank you so much, and have a wonderful summer. See you in September.

1:35:20

Thank you