

Contesting the Foundations of Digital Public Infrastructure – transcript of event recording

Victoria: Hello and welcome to our event on Contesting the Foundations of Digital Public Infrastructure. My name is Victoria Adelmant and I'm the Director of the Digital Welfare State and Human Rights Project at the Center for Human Rights and Global Justice within New York University School of Law. I'm joined by my colleague Katelyn Cioffi, who works with me as a Senior Research Scholar on the Digital Welfare State and Human Rights project. And for the past four years, we've undertaken in-depth research and worked with civil society partners to investigate and highlight the human rights implications of governments' deployment of digital systems. We've particularly studied the impacts of government digitalization projects on marginalized and low-income groups, and our research has documented how national scale systems, including digital identification systems, have served to exacerbate exclusions and inequalities among some of the most vulnerable communities. In today's event, we're going to focus on digital public infrastructure, and particularly the current legal challenges surrounding it. I want to start by giving a quick introduction to this concept of digital public infrastructure in these first few minutes.

So digital public infrastructure, or DPI, refers to large-scale digital platforms that are built, supported, or funded by governments to enable the provision of society-wide services. The key digital platforms that this term refers to are digital identification systems, national scale payments systems, and infrastructures that enable data exchange. These types of platforms are referred to as "infrastructures" because of their foundational nature. They're often compared to physical infrastructures and sometimes presented as the rails on top of which services can be built and run. The idea is that these digital platforms create a solid foundation for other digitalized systems, and government, private sector actors, and civil society can then rely on this cross-cutting infrastructure, leveraging these shared platforms to build apps or digital services. Key to all of this is perhaps the most foundational digital infrastructure, and that is digital identification systems. Digital ID systems allow for the verification of individuals' identity as against large scale databases. These are often seen as the critical first step in building digital public infrastructure because they will underlie countless other digitalized services, such as banking, or healthcare, or social protection.

In recent years, there's been a lot of discussion, for example, about how countries which already had a digital identification "layer" of digital public infrastructure when the COVID 19 pandemic hit, were more able to quickly pay emergency financial aid to individuals. In light of these success stories following the pandemic, today's event comes at a time where there's increasing emphasis and accelerating investment in DPI. We're now seeing many new initiatives to increase support and investment to build out these national platforms, and international policymakers especially are embracing digital public infrastructure. So at the latest spring meetings of the IMF and the World Bank, the director of the IMF stated that DPI is, I quote, "The most effective accelerator of inclusion that there is." And it was agreed that there is going to be, to quote again, "A big push in the next four or five years where DPI will spread very widely."

But there's growing evidence of how the digital platforms comprising DPI are negatively impacting communities at the margins. In many national contexts, the rollout of digital identification systems, and the stacking of other systems and services on top of those foundations, has all too often had serious human rights consequences, and we're going to hear more about these realities throughout today's conversation. In light of the documented harms, many digital ID systems have become the subject of legal challenges. Groundbreaking judgements have already been handed down in India, Kenya, and Jamaica, which have already confirmed the severity of the risks at hand and many other legal challenges are currently underway, which raise a wide variety of human rights issues, from discrimination to social rights deprivations and privacy violations, among others. Clearly there are remaining problems within current approaches to building out digital public infrastructure, and there are some crucial safeguards and mitigation mechanisms that need to be put in place.

So in this event, we're going to look to four different case studies of emerging digital public infrastructures, spanning from Uganda, to Mexico, Serbia, and Kenya, which all have triggered litigation. We're going to hear from experts from the civil society organizations that have been at the forefront of some of these challenges, and we will hear about the issues and the harms at hand in the varied case studies to understand some of the realities of the implementation of these foundational systems in specific contexts. Crucially, this event is going to ask: how might the issues arising in these case studies inform the kinds of safeguards and remedies that are needed within the agenda for digital public infrastructure? What kinds of tools are available to policymakers and what kinds of approaches can be adopted to ensure that digital transformation is built upon a foundation that is truly inclusive and advances human rights?

I'm delighted to now introduce our speakers for today who are going to talk to us about the specificities of the risks and the guardrails needed as DPI has been deployed in their national context. So we're joined by Brian Kiira, who is a program officer at the Initiative for Social and Economic Rights, which is a Ugandan human rights organization, founded in 2012 to ensure the full recognition, accountability, and realization of social and economic rights, primarily in Uganda, but also within the African region. Next we have Grecia Macias, who is a lawyer at the Red en Defensa de los Derechos Digitales, an organization dedicated to the defense of human rights in the digital environment, based in Mexico. Joining us from Kenya, we have Yasah Musa, program manager at the Nubian Rights Forum, which is a human rights movement that advocates for the rights of the Nubian ethnic minority in Kenya. We're also joined by Danilo Curcic, who's a program coordinator at the A11 Initiative for Economic and Social Rights in Serbia, a nonprofit, nonpartisan organization which promotes and protects the rights of individuals from vulnerable and discriminated against groups.

I want to go now to the four specific case studies. If I can first go to you, Grecia, to discuss a case that was just recently decided. So in Mexico, there's been a significant ruling against the government in the Supreme Court, which deemed efforts to create a massive biometric database for SIM card registration to be unconstitutional. Can you tell us about this ruling and its impact? So what exactly was the issue in the Supreme Court case? What were the harms that the proposed digital system would have entailed? And then, secondly, could you also link this and tell us a bit more about the wider context of large scale digital identification systems in Mexico, and how this court case fits with ongoing efforts to deploy digital public infrastructure?

Grecia: Yeah, like you said, it was April of 2022 when the Supreme Court ruled the unconstitutionality of a biometric SIM registry that the government had imposed, again. It was in 2021 that the government presented the bill that created a new SIM registry with biometrics. Just to say that they have tried to do a big database of a SIM registry before, but without the biometrics, so now the new innovation for the government was that they included the biometrics. And we started our advocacy since it was being discussed during the Congress, we saw the initiatives and we saw the implications and the harms it will have on human rights, specifically the right to privacy, the right to non-discrimination, freedom of expression, also even access to telecommunications devices, right? So we started that complaint – we call it Padron Nacional, you know, the registry – and, even though we started since the Congress discussed it, they still passed the bill. And then we did further advocacy and also we made a strategic litigation against this specific SIM registry.

What did this registry include? It was a registry that was created in order to prevent extortions and specifically it included that all people that wanted to own a cell phone needed to give all their biometrics -- because it was that wide in the law, it was to "give their biometrics" -- so that will imply that it will be from your face, to your iris, to your voice, anything, right? And also they were going to have to give name, location... a lot of data that doesn't really, wasn't required for you to get a cell phone, right? So we said like, well, this is really unconstitutional specifically because there was no other way around it. I mean, if you didn't want to give your biometrics or any of these data, you were denied the access to a new cell phone.

So we made a specific *amparo*, which is a constitutional litigation, and we made a draft of the *amparo* and we made also an online webpage that, basically, it was in a way that anyone could just fill their name and only their telephone or give their contact, their telephone number or give their contact of their telephone and to interpose this specific *amparo*. And also we made advocacy, so the specific office, the specific agency in charge of protecting privacy and data protection, INAI, filed, it's called a unconstitutionality action, it has general effects, so they can go straight... directly to the Supreme Court. So we made both lines of, we worked on both lines, like to do the strategic litigation and also to help to do the advocacy so the agency could file this action, and they did. So we continued the advocacy and also strategic litigation, we received more than... it was 50,000, no more than that. It was like 50K *amparo* actions were presented by a lot of people. And actually that was really reassuring for me because we didn't... we tried to explain what was the implications of a biometric database, a centralized database, and a lot of people responded and a lot of people also acknowledged the dangers that this kind of databases will take.

And also when the unconstitutionality action came to the Supreme Court, we filed also an amicus brief that was basically the same document that we did for our *amparo* action. And we specifically make four claims: that it was a violation to the right to privacy and the right to data protection because it wasn't... it didn't comply with the basic principle of consent because they forced you to give all your data in order to get a new cell phone. It also will be pretty dangerous and could be discriminatory for different vulnerable groups, from the basic dangers and harms that comes with biometrics, also and how it affects vulnerable groups, specifically racialized people and women, transgender people and so on, and specifically also migrants, and people that are, of people with low income that sometimes only can have one line per family, and that posed a specific obstacle for them to get these lines. Also because this was the objective to this raised was to prevent extortion. There was a specific article that implied that the people, that... it will be presumed that the one that owns the line was the one that did the extortion call. So there was some risk also about the presumption, the right to presumption of innocence. And also that with biometrics and how they were going to give this data to other security offices and agencies, it brings the risk of surveillance and also to be under the constant scrutiny of law enforcement, they will be also at risk.

So the court, the Supreme Court decided this, like I said before, last April 2022. And basically it ruled that... it only decided sadly on the grounds that it was, it constituted a violation of privacy. It didn't went on to study the other claims and the implications on other human rights. But it was huge because it recognized the sensitivity that biometric data has and how you need to have a really, you need to pass a strict scrutiny test in order to address that, in order to see that the measure is proportional to the final objective that you want to have. And also it establishes that when you are dealing with the massive collection of data, specifically biometric data, you have to have a previous... specifically when it's done by a state actor, you have to have a privacy assessment beforehand. This wasn't, even though this was a specific article that we had in our data protection laws, it wasn't really ever enforced, or we didn't have any interpretation of how to enforce it, and now the Supreme Court established at least some general grounds to it. And also they said that consent is a basic principle for this kind of massive data collection, and forced consent is not consent. So if you cannot have a way to opt out, or to deny, or to refuse to give your data to the state actor, that's not consent. So that's huge, because even though for, I dunno, maybe people who are from Europe are going to be like, "Well, we have this in the GDPR since ages ago, how are you so happy because of these little victories?" For us it's huge because there wasn't really this recognition of the dangers that biometric databases could have on the rights of people, and now we have it.

And that comes at a really special time and specific political moment, because the Mexican government is really in love with biometrics and all biometric technology related and because, I mean... there are states that are establishing facial recognition systems for law enforcement. Also, we have a lot of biometric collection by our taxes, our taxes officers and also they want to establish a new, well, they have established a new biometric

passport, and now they're also wanting to have a biometric general ID for digital ID. So there was a lot of push forward for the inclusion of biometrics by the Mexican government and this is like a huge, like, pause for them and to say, "Wait, you just cannot establish any biometric measure without doing a proportionality assessment and a human rights assessment" -- specifically a privacy assessment, but we believe that it must be a more wide assessment. And also it gives us the recognition that biometric data is really sensitive data. It's not just the same as a password. It's just not the same as any other data.

And that really comes helpful because there's a lot of bills -- like I said before, a digital ID bill is still in discussion in the Senate even though the World Bank has withdrawn their support and their funding for this project, the government is still going forward, well, wants to go forward with this project, specifically. And also there is a lot of bills, for example, a civil registry, a biometric civil registry that basically wants that citizens give their biometric data every time they register some civil act on the civil registry that could be since they were born, since they get married, since they even, for example, rectify their gender identity on their, on their birth certificates even. So this constant monitoring and this constant want to keep collecting biometric data, it's not over and that's, I mean, that's just a political reality that the fight against these kinds of systems is still going on.

And even though we have a really great result with the Supreme Court ruling that gives us basic tools to work with in new bills, like the consent element, the proportionality element, the human rights assessment, it's still a trend now sadly in Latin America that a lot governments are really wanting to promote these kinds of technologies. But these kind of rulings and these kinds of basic standards help us to establish basic safeguards and also to establish what is not going to be legal at any point. For example, for us, we believe that having a biometric centralized database is such a... it implies a huge danger for human rights, it's not even feasible to imagine to have one, right? So, but yeah, that's now the situation and let's see how it goes with further advocacy and litigation strategies.

Victoria: Thank you so much, Grecia. That's really helpful, and already giving us a sense of the kinds of measures that were put in place in terms of thinking about the safeguards and the sort of proportionality assessment that might be needed before these kinds of systems are rolled out is very crucial to today's conversation. And it's clear as well that this Supreme Court victory in ruling out a large scale biometric database is not an isolated situation and there's so much else going on in efforts to deploy other large scale biometric databases. And I want to turn now to Uganda, because this kind of nationwide biometric database has already been deployed in Uganda many years ago. So Brian, if I can turn to you, in part thanks to the excellent research and advocacy that your organization has been doing, the national digital ID system in Uganda has been garnering a lot of attention and is subject to legal challenge. So can you tell us about some of the issues and the problems that have arisen in the context of Uganda's National Digital ID system? What are the main challenges that the government has faced in rolling out the system, and why has the integration of the ID system with programs like cash transfers been so troubling?

Brian: Thank you, thank you very much Victoria. And it was great hearing what Grecia had to say and you know, in certain parts I could see some things that are not unique to Mexico in terms of the challenges that are being faced. But just to say that in Uganda really, it is also yet another case generally of what we would call putting the cart before the horse, because on one hand we are having this aggressive push for integrating the national ID system into access to social services, but yet on the other you find that the coverage of the national ID is not commensurate. So what has been the net effect of this for us, we've been able to notice, has largely been the issue of exclusion and so we've been seeing numerous exclusions of older persons, women, and this is usually in the sectors of, you know, healthcare as well as social protection, as you did hint in the last bit of your question.

And what has really, you know, underlined this dismal coverage has been issues that attend the registration process -- and again, when we were conducting that research that you mentioned, we were able to see some of the lived experiences of, you know, people that during the registration. And just to note that for Uganda, rolling out of the national ID started in 2014/15, so we are yet to see the first batch of national IDs expire, that is starting 2024. And so just also to note that we are at the cusp of rolling out or renewing the national ID to a more modern and smart ID as we've been told. But just to get into some of the issues that, you know, underlie the registration process, you'd find that the process itself was poorly manned and resourced and one of the things that came of this was that then you'd find a very huge population, for example, being served by let's say one registration station. What that meant is that then you'd have hoards of people who want to register, the sick, the frail and those that are not alike are trying to get to the same point. So then what would happen is that there would be frustrations. You wouldn't believe that you could, for instance, that people could take more than three days trying to get to register, and now you're trying to do this at the expense of going on with whatever source of livelihood you would otherwise be applying, so that is wasted time. And at the end of the day, you found that some people got frustrated and did not register in the end.

And I think one of the other things also that, in a way, informed how seriously people took the process was that people did not really get to understand the imperative of having a national ID, besides the reason that would often be thrown around of, "Oh you will need it to vote." So it was particularly for political purposes, and we know that many people, or some people, do not care about that. But then, you know, fast forward and then you are seeing the government slowly introducing this system in the heart or at the heart of access to social services. So then it is at that point that now some people start to run back to see that they get this ID.

But for some it has been a lengthy process. So one of the other things has been around delays. It is, it takes really long for one to, you know, go and register for an ID and ultimately get it. There's quite a bit of time in there. And so that also is yet another issue, but also to talk to the issue of a lack of documentation, because as you're trying to register, you know, most instances they want to have some sort of baseline documentation that corroborates your, you know, whatever you're stating. So you'd find older persons who will tell you that, you know, "a birth certificate was asked of me," people that have probably never even seen what a birth certificate looks like, that was there. And so without some of these documentations again, some other people just said, "it's not worth it," and they totally gave up.

And then there was also the issue of the errors, errors in the registration process. What you will note is that, in rolling out the registration, one of the things we did see is that they got students, largely, to man the registration points. So then what would happen is, when some of the older persons who did not, you know, have, for example, their date of birth known to them whenever they came up for registration, what was bound to happen then is that there would be guessing or estimation of how old these, how old the younger people manning the registration services thought the older person was. And also too bad that most of the people then, the much older ones, they would be using events that already happened, you know, historically, to try and estimate when they were born. You don't expect an 18 year old who is manning that station then to make a proper estimation because they do not know these historical events. So we had very many errors coming through and these errors were either in terms of, you know, the name, or most particularly in terms of the date of birth.

Because now an issue like the date of birth, you know, came to be very central to you being able to access some services like the Social Assistant Grant for Empowerment that is meant for the older persons in Uganda. If you're not eighty years and above, you cannot receive it. So if then your ID shows that you are younger than that, and yet in fact you are much older, you'll still not be able to get that benefit. And now the twist also comes in that at the end of the day, when you try to rectify that error, that is a whole cumbersome process, and I'm not just talking about the financial implication, but in terms of the, you know, the rigors, the

time that you have to take, and also the legal requirements that attend that process. You will not expect people, especially from the rural areas, to be able to follow through. So at the end of the day you find that some still will remain without a national ID because they could not get to rectify an error that was occasioned during the registration process. And we have many of those. Issues of, you know, unofficial costs that again attended the process, we know about them. Those that were illiterate, that also formed a very big sector of our population that, said hey, "I cannot be able to fill out this form, who can help me?" You'll be paying some costs for that. If you're not able to, then you've left the entire process altogether.

But also most importantly, biometric failures. We did see these as well, that you'd find that, for example, when they had to capture the fingerprints, for instance, it was either that the machines were failing on certain days or simply that someone's fingerprint couldn't be captured because over time it has lost its texture, its integrity and as such that person again will be sent away. So that person is also likely not to have an ID and when we also talk about the issue of...

One might think that probably if you do not have any of the issues that I've mentioned and you have a national ID in your possession, then all is clear, but then that is also not the case because you've also seen instances, and again I'll use some of the older persons that that have been trying to access the SAGE program that I just talked about, that you find a person with an ID that properly shows that they're over and above eighty years, but for some reason they are not on the beneficiary list. So it also goes, you know, back to in a way debunk the whole efficiency, you know, narrative... [connection dropped] ... is failing to capture the people that are actually supposed to be benefiting. And on the other hand you'll see, you know, people that have long passed on remaining on beneficiary lists. And again, because the main source of data has been the national ID registration database and we saw still that even during the Covid 19 period that this database was being relied on to be able to give economic stimulus packages and when that was the case, again, the very stories and the troubles that we've been talking about time and again still surfaced. The people who are, you know, not as vulnerable were the ones instead getting these packages.

So that seems generally to be a problem with the system and which, you know, keeps begging the question then, why is government very insistent on incorporating the national ID system in access to these social services? And we've also seen that it is gradually, you know, trying to seep into other sectors like education, and I think that is in itself something that we were able to raise an alarm on and just say that you don't need to do this. We've seen the evidence before that there is exclusion, whether it is in the health sector, I think I also forgot to say, but also in the health sector we're seeing that happening, that people without national IDs were either being sent away from public facilities, health facilities, or they would have to wait in line before they are attended to. So there is this discrimination that is happening that is all hinged upon the possession or not of the national ID.

And I think as Grecia was also saying, for us the national ID now seems to be so centrally entrenched in your, everyone's life, whether it is, you know, registering a SIM card, opening a bank account, it is right there. So it is one that you have to have. And so just to note also as I wrap up is that it is because of, you know, all this and the evidence that we gathered in the research that we mentioned that we're able to take up, you know, government in court, the High Court of Uganda to say that insisting on mandatorily requiring that someone presents a national ID or reliance upon the system itself, because again, those are two different, you know, issues, the possession but also the general setup of the system to provide services, is exclusionary and something needs to be done about it. I think we can get into some of the nitty gritty of what we think should be done about it much later, but for now, that is it from the Ugandan context.

Victoria: Thank you so much Brian. That's really helpful in setting out the whole host of issues that have clearly already arisen over the many years since this has been put in place, whether it's problems with registration, including biometrics, also errors that you spoke about, which are leading to this system, which is

supposed to provide a solid foundation for many other services, you know, that kind of foundation is clearly riddled with exclusions. And it's really helpful that you pointed especially to how older persons are being affected by this as it's being tied to cash transfer programs. And exclusion has been a really central problem in the Serbian government's deployment of a large scale digital platform as well. So I want to turn to you now, Danilo: your organization, the A11 Initiative, has been campaigning against the so-called Social Cards Law, which came into force last year in March. This law was presented as a means of reforming the social protection system in the country, through creating a large scale digital platform which would enable automated decision making. So can you tell us about how these social cards were meant to function and, again, what the main problems or objections to this law have been and who might be most affected by the rollout of this digital system?

Danilo: Thank you Victoria and thank you for the invitation actually to present what is happening in our context. So yeah, as you said, the law on social cards was introduced last year and the idea was that it will make a more just system of social protection in the country. The government said it will address the issue of the error of exclusion and the error of inclusion within the system of social protection, but unfortunately actually the results of the implementation of the law are not that beneficial for the most vulnerable communities. So at this point, we have more than 15% of beneficiaries that were cut from their benefits because of the implementation of the law.

And another big issue there is that actually nobody is really, nobody knows how the system works because it was not made transparent. So the only information we could collect was based on interviews of people working within the social protection system and individuals who are actually trying to get their benefits. So what we managed to do is actually to, we are trying now to explain how the system works with these infographics, which I would like to share if it's possible, which actually tells a bit more about the system itself. So it's 135 different data sets that were collected through different national registries, actually government-run registries, there's the ministry of interior, ministry of social protection, republic fund for compulsory social assistance and all these different services, different registries, which are then combined with data that is coming from internal databases of social protection services. And then both of these data sets are being used for the, actually automated decision making process, which tells the social worker if the individual is still meeting the criteria for social benefits. At this point we have no cases where actually someone got their benefits because of the social card. It only works in a way that actually, it excludes people from getting these benefits. Everything is based on something that is called Citizens' Unique Personal Number, which is the number that is, as I said, actually unique to every citizen in the country, and you get it when you are registered in birth registry books and when you get your ID card and all other documents that are needed for these benefits. And this system is, at this point, not just that actually it doesn't support most vulnerable communities to get their benefits because we also hear this issue of persons who are not even registered into birth registry books, or actually do not have this citizens' unique personal number.

But it also actually excludes people who are not actually able to protect their rights in these processes, because what is happening is that these kind of notifications which are coming through the system to social workers are giving them the orders actually how to sort out the notification actually, how to solve the case. So the notification they would get tell them this person has, I dunno, 100 euros more than they are supposed to have in order to get social benefits, therefore you have to cut them from the social benefits, and that's all. Individuals are not even being interviewed in this system and they don't even have the opportunity to see how the information that is contained in the social card what it is actually this information tells about their specific situation.

So in some cases we just managed to see that actually the system is, of course, there is an error within the system itself, but also there is a really big concern about this, the fact that you cannot even have this effective remedy, because you don't know what to appeal on. Because you just get the information, "social cards tells

us you have to be cut from your social benefits." And this is really creating a lot of problems for the most vulnerable population.

And this is something that we're trying to address with this Freedom of Information Act, actually, our attempts to get to the logic of this system and actually the algorithm that is behind the creation of this notification, which were not successful since April last year when we for the first time asked the ministry to make it public, to make it actually transparent. After a while they decided not to make it public because it is, what they said is it is a matter of property rights of the company that established the registry, even though the registry works in the public domain, but that's something else. We appealed on this decision with the commissioner for freedom of information. We got the appeal, but then actually they decided the same thing, so it's going back again in the process. So for a year and a half, no one knows how the system actually works, other than this information that we could collect.

Another issue that is really important in this case is related to data protection, which is a huge issue there because 135 different data sets is an amount of data that is not collected in any other situation in Serbia. So in any other circumstances, the government does not possess 135 different data sets about individuals. This is actually something that is really concerning. Also the social card collects data of persons who are considered as persons related to beneficiaries. So for example, your ex partner is also, his or her property is actually being analyzed through these social cards. So this opens up a lot of issues around the privacy and protection of like the basic principles of data protection, as the issue of proportionality is one of them.

Another problem, as I already mentioned, is this issue that the social cards are targeting some communities more than some others. For example, we could see that, for example, Roma waste pickers who are collecting secondary raw materials and selling them are being targeted more because actually this amount of money they make out of the collection of the scrap material is now being visible to the system and actually the tax authorities are understanding that every income they get on their account is being considered as income that should be counted as something that disqualifies them from social benefits. Just yesterday we got a case from someone who we represent for a couple of years now who finally managed actually to remedy this situation of unaffordable social apartment, when actually the city of Belgrade, which is the provider of social housing, decided to pay for all the social, for all the actual cost of social housing, which was not affordable to this person. This amount of money actually was flagged up by the tax authorities as an income and this person actually lost the benefit because this situation was remedied because of the error that was already made by another public institution. So this really shows that the idea of having this kind of system which is going to just check data without even interviewing individuals about their specific circumstances and without giving them the opportunity to challenge this data which is contained in social cards, is having a negative effect on most vulnerable population and, as I said, it's 15% of beneficiaries, decrease of 15% of beneficiaries on the national level is mostly actually the 15% of people who are most vulnerable, actually these 15% are the people who are most vulnerable.

And finally I think this is something that is really important and we are trying also to raise this with the government is that, actually this idea of techno solutionism in social protection and this kind of like effective and economically sustainable social protection is something that is not really working because tech solutions are not, actually they are at this point being tools for exclusion of some people. When we analyzed actually who was working on the social cards registry on the side of the government, it turns out it's like 15 IT engineers and one person from the social welfare system, which shows you actually what is the, what was the idea of the whole system. So the government is now with this system also transforming the way how social work and actually the social welfare system should work, should look like, when the social workers are now more working in this IT tool than actually spending time with individuals who are in need of social benefits.

Because of all of this, we tried to actually challenge this law at the Constitutional Court, something similar to *amparo*, I think, if I understand correctly what *amparo* is in Latin America, is like this normative control of the Act. In our case, we submitted the initiative for review of the constitutionality of the whole law. We are still waiting for the decision of the court. In the meantime there was this amicus brief, produced by NYU as well, but also the ESCR-Net members who were interested to support our constitutional court in addressing this issue and actually understanding better what are the implications of this kind of system.

We are still waiting for the court to decide on the case and at this point what is the most concerning is that actually that even the idea of suspending the implementation of the law until the court decides is not going very well. So we are still waiting for the court even to say something, at least something, about the legislation. At the same time, we have a number of cases where people are losing their benefits because of the social cards, and in most cases they don't even appeal because the access to legal aid and access to remedies is not that easy if you are coming from extreme poverty, as we all know. At this point we think it's, yeah just maybe we can discuss this in Q and A or actually after, if there are like more interest into this issue. I think this is like generally what I wanted to share from our experience.

Victoria: Excellent, thank you so much Danilo, especially in setting out how there have been quite a few different legal challenges and there's clearly different routes here in, kind of going towards the freedom of information commissioner, and also constitutional review, and then individual cases as well, so that's really helpful, thank you.

And in fact in Kenya there have also been numerous legal challenges, also through kind of different avenues, challenging the national digital ID system, which is called the Huduma Namba system and these legal challenges have raised many different issues relating to constitutional participation, privacy, data protection, exclusion, and discrimination. And added to that, recently, questions have also been raised about the role of private sector companies, including foreign biometrics companies which were involved in building the digital identification system in Kenya, as well as in many other countries around the world. So Yasah, if I could ask you to tell us a little bit about the context in which the digital ID in Kenya was rolled out and what some of the risks associated with this digital ID system have been for the communities that you work with? And secondly, I wonder if you can kind of connect that to the role that private companies have played in helping to build some of these digital identification systems?

Yasah: Thank you so much Victoria and Kiira, Grecia. All your presentations were nice. I don't even know where to start with, but when we talk about the Kenyan context, I work with the Nubian Rights Forum, which is a marginalized community based in Kenya and this community has been working tirelessly through the legal empowerment, working with other communities to ask the Kenyan government to really allow them to access documentation, and these documents are some of the things that minimizes them from getting access to services such as health, you cannot get scholarships, you cannot get passport, you cannot get identification card, without being recognized as a Kenyan. And this is one of the things that Kenyan Nubians have been facing for the past so many years.

So when you talk about the issues of digital identity, this is a Nationally Integrated Management System [NIIMS] that came into place through a change that was made through Registration of Persons Act via a miscellaneous amendments bill of 2018. And when you look at these miscellaneous amendment bills, they are made to just divert information, small amendments, but when you look at about issues of NIIMS, this is a big project that was brought into place, collecting of data. The reason why we decided to go to court to challenge this issue was about the issues of data protection. The Kenyan government had not really come up with a good data protection that will be able to protect people's data.

The issues of public participation. There was no public engagement when this government, when the government was coming up with digital ID, and this really affected so many people because there was no

clear information on when registration is going to stop, when, if you have not registered for this mass registration, will you be given an opportunity for you to re-register next later? So these are some of the issues in exclusion of the minority groups because, for you to have registered for the Huduma Namba you needed -- Huduma Namba is another name of the digital platform, the National Identification Management System -- so for you to register for this, you needed either ID, passport, driving license, or a birth certificates. And these are the documents that communities who are at risk of being stateless are looking for so that they can be able to get these services. The Kenyan government also wanted to link the digital ID with services whereby Kiira talked about the issues of, Ugandans not accessing services, such as health-wise.

So these are the things that we really wanted to highlight, because without this document you cannot be able to get access to services. Children, we've seen so many, not only the Nubian community, but other minority groups, without getting documentation. So if this was to replace identification card, there are so many issues that we really wanted to make sure that they're able and they're being linked out.

Talking about the private sector, I'd like to mention a little bit that we filed a case in France, together with Data Rights, challenging the export of biometric equipment for NIMIS under the French due diligence law. The case, the challenge specifically was around the lack of safeguards for the export of equipment to harmful human rights. And the case was filed in December. We got a judgment where the judge had asked to have mediation talks, which is still confidential and I will be able to share with you the information about this later on.

But to speak more about the issues of data in private sector, biometric technology is de facto dual to use technology and can lead to grave human rights abuses. So we have to make sure that there is cooperation between private sector, the public, and the government, whereby then collection of information is minimal. We need to understand how this information is going to be used. We need to understand how are they going to make sure that they protect people's data. For instance, in Kenya there has been a lot of scrutiny whereby the Kenyan government are using information to scrutinize people. Sometimes looking at this digital platform, by press of a button you can be called Al-Shabaab, because all of the information that they have, it's easier for them to just press a button and you are linked to something. So we have to make sure that there is a comprehensive data protection into place, there is inclusion of the community, there is public participation so that at least the issues that are being discussed are things that we can be able to push more forward.

So I think these are some of the issues that really made us go to court to make sure that, at least, data protection is in place, inclusion of communities that are at risk are in place, collection of information: the government needs to take what they need, not everything, because when you take all the information, the information becomes uninformed information because you're taking everything about someone. So these are the things that we really wanted to make sure that the government is actually doing its work and it's actually making sure that they're giving information to the community. I wouldn't really talk more about this since we are behind time and I think if there is any other information then we can be able to share it later on. Thank you Victoria.

Katelyn: Thanks so much Yasah for that great outline and it's really nice to hear about a case that's currently in progress and I'm sure a lot of people in the audience are interested in following that development and seeing how things pan out. And many thanks to all of our panelists for these really illuminating case studies, I think they really show some of the complexities of using things like digital ID systems and digital public infrastructure, particularly in programs of social protection and other forms of public services. It's now my real pleasure to introduce our keynote speaker, Nanjala Nyabola, who is a writer, researcher and political analyst who has been doing vital work critiquing the digital transformation. We're really honored to have Nanjala here today to give our keynote speech. Nanjala, we've heard these four really diverse case studies that have highlighted different human rights concerns, ranging from privacy and data protection, discrimination,

and exclusion from social protection, access to information, and the involvement of private sector actors, to name just a few, and we've also heard a bit about some of the proposed remedies, safeguards and mitigations, including the content of these ongoing legal challenges you know, that are asking for things like consent based models, allowance of alternatives, proportionality reviews, data privacy and human rights impact assessments. So I wonder if you could help zoom us out a bit and discuss what you see are some of the key trends here. Could you reflect a bit on the kind of the broader context for the introduction of digital ID systems and digital public infrastructure, and maybe share some thoughts that you have about the effectiveness of some of these tools and also the major challenges that you see going forward to try and encourage a more human rights oriented approach for both digital ID systems and digital public infrastructure more broadly?

Nanjala: Thank you, Katelyn. First of all, I wanna apologize if my internet breaks up in advance. I'm traveling so the connection might be a bit flaky. I just recently have been reading a lot of Milan Kundera, and for those of you who are not familiar with Kundera, he is a Czech writer who left the Czech Republic during the communist era and moved to France and now identifies as a French writer because of some of the things that he lived through and experienced in the Czech Republic. And one of the things that comes across really strongly in Kundera's writing is how insidious the police state was in the Czech Republic during the communist era and the elaborateness of the surveillance state and the surveillance economies around that. So the ability of secret police to show up at someone's church, you know, to show up in people's romantic relationships, to show up in people's personal lives.

And I think... the reason I bring this up is that there's always a human element to so many of the things that we talk about when we talk about digital technologies and surveillance tech and all of these things that gets lost. We get stuck in technical conversations, in, you know, these nitty gritty, rubber-meets-the-road kind of conversations and we lose sight of the human dimensions of the things that we build. Technologists are very good at losing sight of the human dimensions of the things that they build. I think someone has just mentioned on this panel, you know, you have a new digital ID system being built with 15 IT people and one social services person. I mean that's really telling of where the governments that we are talking about, where the governments of the day see the problems and where they see the solutions.

So in zooming out, I would group the challenges that are arising with digital ID onto two levels. One are the technical conversations, and the other are the normative conversations. And I'm gonna just go into a little bit of detail about each of them. To start with the technical issues, because I think the technical issues are kind of the easier problems, these are the problems that can be fixed by having, you know, a different type of IT person in the room, by having a different type of AI specialist in the room, by having a person who is a technical expert who has a slightly different understanding of what needs to go into these systems. Some of these are, you know, encompassed in the litigations that we're talking about. When I hear about the Ugandan example, the first question that I ask myself is, "how can an identity expire? How does a person's identity expire? How do you stop being the same person that you were when you signed up for the ID system?" That's a technical question that needs to be addressed, you know, that can be addressed by having a different kind of ID specialist in the room. An identity is something that should endure, that is attached to a person, that should be something that follows them through their life in a specific society. Charging people for ID cards, charging people for participating in what really should be a right, you know, the SDGs and when they say that everybody has a right to a legal identity, the idea is that, it's a fundamental right. It's not something that you... the government should be able to exclude you on the basis of your financial ability, on the basis of your access, you know, your ability to walk to the ID system and yet in Kenya, to the registration place for example, and yet in Kenya for example, we've seen this repeatedly, people with disabilities being unable to sign up for ID systems because the person who's signing them up did not make accommodations for people who needed wheelchairs. We've seen this with electoral registration system, digital electoral registration

systems. We saw this with Aadhaar, with people who handle, you know, farming equipment, with people who handle hot objects, who lose their fingerprints by virtue of the labor that they do, to keep these economies afloat, being then unable to participate in the digital ID system. So charging people, excluding people on such technical matters, this is a technical issues that can be addressed by the kind of technicians that we have in the room.

The discrimination question, right? Excluding people by virtue of their identities because these are identities that are "unwanted" or viewed as "unworthy" by the state. These are the issues that we're seeing arising in Kenya with the marginalization of the Somali people. These are things that we can litigate easily because these are technical, easily, relatively easily, because these are technical questions on how we interpret who belongs in a specific national context and who doesn't belong in a specific national context. But the discrimination issue, I'm gonna come back to that because I think that straddles both lines. It's a technical issue that reflects the state's perception of who the citizen is and what benefits the citizen should accrue by virtue of their identity and their presence in the polity. But it's also a normative question because there's questions there about how we understand who specific people are.

Datafication, right? This idea that we're going to collect every single possible data point on a specific individual and have it track them through life. The example that I always come back to in comparing, why do we complain about, for example, national ID cards in Kenya, Huduma Namba in Kenya, and not about passports in Kenya? Well, the passport is also a digital document, but it serves a very narrow function. It's not collecting every single possible data point about you. It's not something that, you know, is designed to shape certain experiences of... you know, if you have a valid passport, you are able to cross the border, but the passport doesn't say, for example it doesn't collect ethnic identity, my passport doesn't collect any information about my ethnic -- it doesn't try to define me by specific ethnic markers. It doesn't try to define me by my geographical location. You know, I, as a Kenyan citizen, I am technically able to get a passport wherever there is a passport registration site. I can go wherever there's services available, but your ID card is something that you can be told, your Huduma Namba is something that you can be told, "you don't belong because of your ethnicity in this specific geographical location and therefore you are not entitled to apply for your Huduma Namba within this specific geographical location." So this idea of governments collecting these massive amounts of data to link them to a specific definition of what an identity is, this is also something that is, you know, a technical question that has very specific social consequences.

And of course the safety and the security issue. You know, they wanna talk about cybersecurity as a very highly advanced sort of complex thing which, you know, in some ways it is, but we've seen year on year on year, these massive government databases getting hacked, because once you collect all of this vast information and link it to people's biometrics and link it to people's identities, and you put it on a database, you are immediately creating a security vulnerability and that security vulnerability is going to require constant financial investment to stay ahead of hackers. We saw the tax database in Hungary, I believe, was hacked. We've seen massive ID databases getting hacked and all of these vulnerabilities. People's privacy, people's ability to exist being compromised simply by virtue of these massive data collection exercises. So safety, security, these are also technical questions that are embedded.

There is, however, this secondary level of vulnerability that is, I think, implied by all of us who are gathered on this call, and those of us who are approaching this from a much more human, a much more social, rights, civic-minded approach. We're not just interested in getting technically sound databases. We're not just interested in issues of, you know, the data set is... or the data is collected and kept in the most secure vault. Even if it was in the most secure vault, even if it was done to the highest technical standard, there's still deeper questions about digital ID that we are trying to get to the heart of, that are really, really important to addressing the justice issue.

The first and the most important for me, at least, is the question of informed consent. What are people agreeing to? How are people being brought into agreement of these issues? As you heard from the Kenyan presenter, the Huduma Namba in Kenya was pushed through under a hail of coercion, the people were being told, if you didn't sign up for this thing in the next 28 days, you would essentially lose your right to exist within the civic space as a citizen. You would not be able to get a passport, you would not be able to register deaths, you would not be able to register births, you would cease to exist. And that kind of governance, it points to -- it's not just the question of how the ID was done -- it points to the relationship between the citizen and their government. What is the government trying to accomplish by rushing through these initiatives? What is being accomplished by the fact that people are not being given a chance to understand the implications of the systems that they're being asked to subscribe to? It's about civic relationships, it's about the social contract, the fact that the social contract is something that should be entered through voluntarily and that people should be able to opt in and opt out of based on the changing circumstances.

At the heart of all of these digital ID systems is a really important presumption, the presumption that citizens trust their governments, but the vast majority of us live in societies in which we don't trust our governments. We can't trust our governments, because the biggest violator of our human rights, of our civic rights, is the government itself. And so this is not a question that can be merely addressed by building digital ID systems to the highest technical standards. This is a question that is addressed by having really strong human rights evaluations that precede, you know, the rollout of the digital ID system. It's about participation. Was there adequate civic participation and not just this illusion of participation before we launched the digital ID system, that people were actually engaged at multiple levels with the process of building and of rolling out the digital ID system.

I always come back to also the second point. The question of resourcing. How do we pay for these digital ID systems? What is not being done in the process of building the digital ID system is just as important as what is being done. When a government allocates \$60 million to building a digital ID system, which is what happened in Kenya, and then turns around and tells you "We can't afford to pay for primary school education. We can't afford to pay for, you know, basic healthcare. We can't afford to pay for X, Y, Z." There is a tension there in, you know, which can be broken down to, well, what is government for? What is government for? And increasingly as international multilateral organizations foist these digital ID programs onto countries of the global majority, countries that already have very tough economic decisions to make, we're seeing these trade-offs having very serious implications on people's political lives. Right now, the Kenyan government, again, has spent all of this money on the Huduma Namba and then is telling civil servants, well, we can't pay your salaries. Has spent all of this money on these initiatives and then is telling, you know, people... The Ugandan government, you know, "we've spent all this money on this digital ID system and you have to bring in money, through digital ID, but then you can't have meaningful reforms to the education system." These are very real trade-offs that are being foisted on developing countries, on countries of the global majority, that also have to be contemplated when thinking about these digital ID economies and the political economies that they make possible.

The other normative question is this question of identity. How are we defining people's identities? How are we conferring identity onto people and how are we taking it away? Some of these digital ID systems are built on the premise of reinforcing the systems that were there before. If the system that was there before was patriarchal, if women were not able to pass on their IDs to their children, if women are not able to register their children because their father is absent, because the father does not claim paternity, that raises a discrimination issue. If the question of ID is about hardening ethnic identities that people themselves don't see as that hardened, right? Again, I go back to the Kenyan example, the inheritance of an ethnic... the fact that an ID system implicitly collects ethnic data and then says you can only inherit your ethnic identity from your father, creates a moral paradox for people who live in mixed, people who live with mixed ethnic

identities. People who haven't made those declarations of themselves, who very much see themselves as both, who very much see themselves as existing across these lines, and then being told by the state that "No, you have to pick and this is where you belong" and in the Kenyan case it follows you generationally. That ethnic identity is something that, what is contained in our ID cards is not how I identify myself. It's not even how my father identified himself. It's how his great grandfather was identified by the British colonial government.

So this hardening of identities has consequences. When we think about how the National Population Register was implemented in India, in Assam, it's not just about this hypothetical, you know, it's not a thought exercise. When you tell people that because the ID card says that you are this and not the other thing and that it follows you indefinitely, that has consequences on access. You know, if you are an ethnic minority living in a specific... we heard in the Roma context for example, you are an ethnic minority living in a specific geography in which your access to resources is tied to the way the state identifies you, this hardening of ethnic identities is not just a thought exercise, it has real life implications. And so we have to engage with it, not just as a technical question, but as a normative question that influences the way these ID systems should be shaped.

This other question of the scarcity mindset, the efficiency question, this very management consultant approach to what government is for, that the most efficient government is the one that has the most information all the time, that is able to get that information very quickly. I always wanna ask, what if what the government wants to get efficient at is inflicting violence on its own citizens? What if what the government is trying to do -- and this again is not an abstract thought question -- we have in Kenya these security cameras that were launched and were put in many public roads. So there's always this constant data collection that's happening on the major thoroughfares in Nairobi, Mombasa, and there's big data centers where people, police officers are constantly watching these cameras, and the idea was that it would make crime fighting more efficient. What has happened instead is that it's become more efficient at finding critics of the state, but if you criticize the government, these systems of surveillance make it such that the information, once you have that license plate, once you have that little piece of information, being able to track people, you know, through all of these various databases, critics... when someone tweets something that is against the state, that the police can show up at their house, you know, within the hour. But if your handbag gets stolen while you're standing underneath that camera, suddenly the cameras don't work anymore. These are paradoxes that many of us are contending with as we are being told that efficiency is good, that more data delivers more efficient government, that smart cities deliver more efficient government. Well, is the reason why these social services are not being allocated to people, the fact that they don't have digital IDs or the fact that the government did not want to allocate them those resources in the beginning? That's not a technical question. You can't engineer that. The solution to that question, that is a political question, that is a social question, that is a normative question that must be engaged with before we provide these questionable governments with this tremendous capacity for collecting, sorting, ordering people, giving people, allocating people's identities and thereby allocating people resources from the state.

The promise of efficiency, the illusion of efficiency, this is very hollow to me, because I think that there is, there's a scarcity mindset that is very false. That idea that we are told on one hand that... I think it was, I think it was actually Bill Gates who said this, that human beings are more prosperous than they have ever been throughout history. Then why do we need to put all of these barriers between resources and the people? Why is it that it's harder for people to access free healthcare in 2023, which is supposed to be the most prosperous time in human history, than it was, you know, in 1963, 1973. What is the mismatch between the available resources and the people accessing them? It's not purely an efficiency question. There are political questions embedded in that. There's a scarcity mindset that's embedded in that, that is worth unpacking.

And finally, you know, we've already had this idea of techno solutionism and this is tied to the idea of efficiency. The idea of throwing technology at complex social problems without taking the time to unpack

what the social... what is the origin of these complex social problems, ultimately leads to more predicaments. And think about the refugee ID systems, the ID systems that are following refugee and migrant populations around the world. Violence that people are enduring at the border because of the lack of ID documents, because of the way in which the state chooses to see and categorize these identity systems. Is the reason why refugees and asylum seekers in some of these western countries are being denied access to critical services, the fact that they don't have digital IDs? Or is there political choice to make the digital ID an obstacle to accessing these resources from the state, right? Is the fact that people are not making... is it that refugees and migrants are not making themselves available for ID systems? Or is it the fact that ID systems are being used as a barrier to keep people out, higher and higher threshold of identifying yourself, as a person who fled, who didn't carry, you know, their passports and their ID documents with them when they were crossing the ocean? So there's a contradiction that is embedded in techno solutionism. It distracts people I think from more important issues that need to be addressed.

I think about the Afghan case quite a bit. In Afghanistan, before the allied troops, before the Western allies sort of pulled out of Afghanistan, they had already built this very elaborate digital ID system, the e-Tazkira. You know, Afghanistan to be fair, had been going through multiple cycles of warfare over many years and had not conducted a census, had not conducted ID registration systems for multiple years, for multiple decades, and so there was this big effort to build this digital ID system for the Afghan people. And it was World Bank funded, it was technically very sound, although there was a lot of questions Afghan people raised. The idea of "Afghan" is actually a loaded concept. We from the outside kind of look in and say, "well of course that's your nationality." But of course there are ethnic questions where ethnic minorities within the Afghan population for whom that's not merely a national descriptor. If you are a Sikh living in Kabul who has endured ethnic marginalization, there are questions there. There's a history there of back and forth of exclusion, of marginalization, that makes people say, "Well I don't know if this national identity adequately describes who I am ethnically and what my relationship to the central state is." So there was all of that, but then there was also the question of this amazing, elaborate, very detailed data collection, digital ID system then being handed over to the Taliban when all of these forces withdrew. So now the Taliban is sitting on all of this information. Is that a technical question? Is that a normative question? Would that have been addressed by having more IT people in the room?

I want to stop there because I know I've been going on for a long time, but I really wanna leave you with all of these things to think about. Sometimes the IT people want to convince us that if they address all the technical questions then the ID systems will work fine. But what we've heard from the presenters here today and what I think all of these examples are showing as they keep coming up is, there's more to this than simply meeting those high technical thresholds. We have to think deeper about why it is that governments are building these systems and what their implications will be. Thank you.

Katelyn: Thanks so much Nanjala and I think that framing is really helpful to some of the really big questions that are being asked by the panelists in their legal challenges, in their advocacy work about the purpose of these systems -- what they're meant to achieve and what they're actually doing to our societies. So thank you very much for that really enlightening talk.

We're coming up on time and so I want to end with a lightning round of questions or rather, one big question to each of the panelists that kind of draws on what Nanjala was just saying and it's maybe a bit more mechanistic, but it's really asking, where do we go from here in the light of these big challenges at both the technical and the normative level that we're facing? What do you see as some of the most urgent priorities and some of the available pathways that we have, to introduce new safeguards, to include mitigations and remedies in some of the systems that are kind of running forward at an incredibly rapid pace? And I'll ask you all to limit your remarks, to just give one or two examples of kind of more concrete pathways that you see that need to be taken advantage of, and these could be addressing some of the technical questions or they

could be more aimed at some of the normative questions than Nanjala has raised. And I'd highlight that in the Q and A, you know, people are asking about whether there need to be new pieces of legislation, whether there should be the introduction of punitive measures for public and private actors? We've heard today about impact assessments and also about consent based models. So for each of the panelists, maybe, you know, there's a huge universe of alternatives here, but could you give us an example or two of what you think would be the most urgently needed interventions in this area? And I think we'll go in the same order we did in the first round. So Grecia, if you could perhaps start us off.

Grecia: Yeah, like basic frameworks of safeguards, so around privacy and data protection, specifically when we're talking about consent, it's essential for any other kind of digital public infrastructure. Also before, maybe before that, to really assess what's the final goal of it and to see if that's even compatible with the human rights law at the first of the human rights, or to establish basic... basic assessments and human rights assessments, and how to do this assessment, I think are the most urgent things to, to not develop tools or any more infrastructure that is going to harm people. I think those like really concrete measures.

Katelyn: Yeah, thanks very much. Those are great examples and I think also tie back to what you were talking about in the Supreme Court case and what actually the court was demanding in some of those aspects. Brian, would you like to add on from the Ugandan perspective?

Brian: Yes, thank you. Thank you Katelyn and it was great hearing the things that Nanjala really had to say that tie into, you know, the realities that we're facing. But also just to say that for us, again, ours has been around saying we need to build a national ID system -- if we really need to -- that speaks to the realities of the people, but also serves the people. So we shouldn't push this machine that is not serving the people. And one of the things that we've said is that, in our context, we've seen since time immemorial that we've had, you know, ways or alternatives of identification that have for long worked, and at this point, if we are to do an analysis, we clearly see that the narrative of efficiency hasn't been working well and as such we're just saying that we do need to let people use other alternatives that we've used before to access social services. Someone shouldn't be denied just because they were not able to get an ID and then they cannot have access to healthcare, or to education, or to, you know, social protection. So for us it is: let's have other alternatives as you get your act all together. So that is it for us.

Katelyn: Yeah, thanks Brian and that importance of flexibility and alternatives I think is something that's come up quite a lot, and the rigidity of some of these systems is inherently problematic. Danilo, would you like to come in?

Danilo: Yeah, thank you. I would just add actually to something that Brian said, that if we can imagine like the perfect world where everyone is included, and actually there is everything is working, like there is no issue of ID, whatever we actually spoke about, I would really like to then actually go to like another step to just think about if actually we can say that our legislation is made for automated decision making processes now. So we are just using this automated decision making processes as a tool for legislation that is never actually meant to be implemented in a way with that. So we have to actually restructure the way, how we want to think about it. This is just a tool that is also changing the way, how we access these rights from the public domain, which is something that we're not supposed to have in this case. So to kind of like to open up this discussion about actually substance of this, where these tools are being used and actually if the algorithms and the automated decision making processes could be used in legislation that is, that we have now in this, in different legislations, yeah, different jurisdictions.

Katelyn: Yeah, thanks Danilo, clearly the importance of dialogue is also a key theme here in really reevaluating and re-critiquing and opening up those conversations that some are kind of seeing as already closed. Yasah would you like to make our final intervention here?

Yasah: Maybe for mine is just to make sure that at least the government should address the issues of exclusion. They have to make sure that everybody's included. They should not be linking digital ID with services. They have to make sure that at least when you're about to go to hospital, it is not the document that is preventing you from going to hospital. They should also be able to make sure there is an extensive public participation because the public really needs to really understand what they're getting themselves into. They really need to know everything about digital ID. The issue of minimization of data, let's collect what we need, and let's not collect all the information. The decentralization of the digital ID. When you look at the Kenyan system, the digital ID is centralized whereby it means all the information there is stored in one particular place. But decentralizing makes it easier for your information not to be manipulated by a press of a button, not all of your information will be violated.

And then we really need to work together as multi-stakeholders. This is not only the issue of civil society, this is not only the issue of lawyers, this is an issue that affects each and one of us. So we have to make sure that we come together to discuss about these issues. And lastly, we have to make sure we sensitize the lawyers, we sensitize the community advocates, we sensitize also the judges, because they really need to understand what they're dealing with. Because if you don't understand what you're dealing with, then it is very difficult to make a sane judgment. And also the last one is, let's make sure that we hold the government accountable and use other platforms because the challenges that we've seen on litigation is the processes, all the information that are taken by the government, by the time a judgment is made, there is a lot of harm that will have been made. So let's make sure we use other platforms such as community advocacy, legal empowerment, to work together with this government for a better future when it comes to digital ID. Thank you so much.

Katelyn: Thanks Yasah. I think it's clear, you know, while litigation has played a key role in all of the case studies that we've discussed today, that it's not the only tool at our disposal and that there are a lot of other avenues for achieving some of the changes that we would all like to see in some of these systems. So thanks very much for that. And thanks so much to all of our panelists today for sharing their time and expertise with the audience and to our keynote speaker, Nanjala, thank you very much for your critical insights about the kind of big picture issues that are at play here.

Although I think it would be incredibly difficult to try and summarize such a rich discussion, I want to outline just a few key takeaways today before wrapping up. The first is really the importance of what Nanjala referred to as the human dimension. You know, while digital public infrastructure and digital ID systems are often seen as foundational, it's important to remember that the true foundation for such systems already exists. It exists in the political systems, in the trust or the lack of trust that individuals have with their governments, in the strengths and weaknesses of existing human rights protections, in existing social work programs, and it exists in the economic marketplaces, relationships, and structures that affect much of our everyday lives.

The second takeaway is the really urgent need to safeguard the rights of those who are on the margins and to make sure that these systems work for them and not against them. This, I think, should always be a guiding principle, but it is especially important when such systems are deployed in areas of social protection and social welfare, where persistent discrimination threatens the very essence of such programs and should be eliminated immediately.

The third and final takeaway is the need to integrate safeguards, remedies, mitigations, and critical discourse throughout the lifecycle of any digital infrastructure program. I think it's never too early and it's never too late to start some of these discussions. And while the examples that were given today by some of the panelists of

remedies, mitigation, and safeguards, may not solve some of the structural normative challenges or guarantee truly inclusive systems, they're at the very least a good place to start.

And Victoria set the stage for today's discussion by talking about the term digital public infrastructure, and it's something we've reiterated a number of times throughout this talk, and its growing salience in policymaking circles. And we can see the growing impact of this concept in the way that it's talked about in international forums, such as at the World Bank annual meetings or in the discussions around the UN Global Digital Compact, but we can also see the growing interest from national governments themselves who are making moves to transform these concepts into reality and export things like the India Stack model, which is one of the most advanced examples of digital public infrastructure.

So we really want the conversation today to serve as a salient reminder for all policymakers, for all individuals and communities who might be affected by some of these systems, for civil society, for academic researchers, for everyone, because these are systems that are really going to affect a lot of people -- and we really want to emphasize that if digital ID is to be the base for new stacks of digital infrastructure, then a reckoning of what works and what doesn't work at this very foundational level should form the basis for all of these ongoing discussions.

So with that, I'll wrap up this session. Thank you very much everyone for joining us today. We look forward to continuing these discussions and encourage you to follow the work of all of our panelists and speakers today. Thank you.