Eric: Hi. So before introducing our episode with Suha Muhammad today, I'm just going to take a seconds on the events that led to the precipitous drop in the crypto markets last week. Now I'm not going to restate or analyze those events, and I'm not gonna do much more than just note the challenges that risk assets generally have during periods of fed reserve tightening.

But I am going to state this: The Encrypted Economy isn't about the market's crypto going up crypto going down, and it's not even a crypto podcast per se. It's about the ecosystem that is the encrypted economy, and that is not going anywhere anytime soon. And it may go through periods of expansion and contraction, but this whole space is just going to grow over time.

And my job here is to just help you, the listener understands the forces that are shaping it. So back to this week's episode, which is with Suha Mohamed talking about some of her work at the uptake Institute at an India. Now they are a policy research Institute. They focus on matters and questions like, what are our personal digital lives?

How is our workforce going to evolve when things are changing in technology like AI, or how are emerging technologies going to impact our relationship with the state questions globally, quite frankly. So for whatever reason, the first few minutes of this episode were lost. We didn't have a chance to retape it.

So we're just going to cut out some of that and just launch into the first question. So I hope you enjoy this episode.

Welcome to The Encrypted Economy, a weekly podcast featuring discussions exploring the business laws, regulation, security, and technologies relating to digital assets and data. I am Eric Hess, founder of Hess Legal Counsel. I've spent decades representing regulated exchanges, broker dealers, investment advisors, and all matter of FinTech companies for all things, touching electronic trading with a focus on new and developing technologies.

Now AApti is located, its headquarters is based in India. And, but it is a global focused organization.

So today we're going to talk we're going to try to shed some light on things in the Indian, within India and then how they relate to the broader international context. What do you see as some of the cultural differences towards data privacy in India versus the US, Europe?

Suha: I think it's interesting.

When we're looking at cultural differences and attitudes and there's something significant in the Indian context to consider. So in 2017, privacy was recognized as a fundamental right, and I think that's significant because it really does exalt its status and the way that we should be thinking about it as something that needs to be protected as one of the highest levels of freedom

or rights that we have in this country. But at the same time, there isn't necessarily an overarching privacy legislation or regulation that actually ensures that these rights are protected. And so I think there's a bit of a tension there because there is definitely a recognition that this is something that needs to be protected for all citizens, yet

I think in terms of the efforts to regulate it and efforts to protect our right have been a challenging journey so far. So I think there's definitely been influenced from what we've seen from GDPR in Europe. And how that framework has led, and trickle down into our understandings of privacy.

I think also at a community level, there've been various incidents where, Indian citizens have been made aware of, how our digital rights have been imperiled in some ways. And I think, this has been a cause for concern. Most recently also with the Pegasus spyware case that came up, I think across the world, I think citizens were extremely concerned to see that surveillance can be done not just by private entities, which we're now used to and maybe potentially too comfortable with but also by state actors.

And so I think this brought up, concerns and the way that we're framing. We recognize it's a right, but there are concerns in which, you know how does this actually translate into practice and what does that look like on ground? So I think we've seen some progress also in terms of the drafting of, potential personal data protection bills, but this has been going back and forth for five years now. What's interesting also in the Indian context to note which might be a little bit more cultural is that. GDPR and perhaps others Western sort of recognitions of privacy tend to be quite individualistic. So you're considering sort of individual data rights and protections.

You're looking at consent also from a sort of individually. Individualized view, and I think the nature of data is that it tends to be quite relatable, and you can gain significant value when you're sharing it. And also when you're aggregating it from different sources and there's a significant community angle to data, it doesn't just relate to one person. It relates often to many people. Any decisions that are made around data, they can extend to communities and groups of people. So what we saw in the Indian context was a non-personal data governance framework was released, and at that point in time, it actually recognized the community element to data, which was quite interesting.

And in a way that. It saw that individuals should have community rights over data and that could be exercised potentially through a nonprofit that could serve as an intermediary in that position and make sure that the community was aware, had the necessary literacy around what data was valuable, how that could be used and how that sort of value could be derived. So I think those are the sort of cultural nuances and context that, that make India quite an interesting space to look at how privacy has evolved and how we're looking at it. We also ran a very interesting campaign and one of the first sort of large consumer focused campaigns to shed awareness on privacy that we ran with the supportive Omidyar Network in India.

And I think the biggest learning for us was that I think as a result of global conversations on privacy, whether it's through documentaries, we're seeing on Netflix or otherwise, there is a cultural acceptance, at least through, at least from digital natives, that privacy is a huge concern. Yet it remains to be something that people feel quite defeatist about.

So it remains to be something that people say, okay platforms have my data. I don't necessarily have control over it. What can I actually do? We don't have a privacy legislation. And we understand that there isn't necessarily a lot of accountability that we can demand for from platforms at this point in time.

So I think taking that into account and being aware of that context and also being aware of the nuances of how these structures play out specifically in the global south, in countries like India, for instance Aapti was very keen on looking at, elements around sort of data sharing

that seemed to be quite well-rooted and quite well understood. And looking at frameworks of data governance and saying, how can we extend the way we think about data governance beyond just compliance to consider the individual who's often the data subject from whom data is being gathered and captured, but tends to be absent from these conversations around how data is collected, stored, use shared

with whom it's shared and for what purposes. And so that's led to our broader focus on looking at how this framework can unlock data, incentivize sharing between, multiple users and a sort of digital intermediary, which can be an existing organization, can help whether it's individual communities help represent their digital rights in, in, in a way that's a little bit more meaningful and really put them at the center of a lot of decisions that are made around data.

A lot of the concerns around data misuse can also then be mitigated potentially through this kind of a structure as well.

Eric: Interesting. We had a while back; we had a podcast with Dr. Jennifer Cobbe and Heleen Janssen from Universities of Manchester and Amsterdam. And we talked a lot about a figuration analysis of privacy.

Basically it's a human network and as opposed to just a purely individualistic and how it relates to the state, that there are communities that there's these complex networks and all that needs to be taken into account when contemplating legislation that impacts privacy, because I think as you note, sometimes, the individual

may not be as represented, they can't be as represented, and if you're asking them to take charge of their rights that may not always work either. So you have to think more broadly, like how do they get their rights represented without necessarily having to take action themselves, or having to assert their own personal rights as part of a broader community?

Interesting. And I think that feeds a little bit into another topic, which I think privacy folks focus on which is, I don't know if I'm pronouncing it right, and you'll pronounce it right, "Aadhaar." Could you explain what that is? The impact on Indian society and how that factors into a privacy as well as an even a data stewardship analysis.

Suha: Sure. So I think, so it's pronounced Aadhaar and other essentially was a, or is a sort of 12 digit number that is generated by the, I believe it's the unique identification authority of India. And it has been compared to say the, like a social security number in the US. And the idea is that this 12 digit numbers connected to two sets of, That, pertain to you as an individual.

This includes biometric information, as well as other demographic information, like your date of birth, your phone number, your address, et cetera. And so when this sort of initiative or scheme was rolled out, the sort of vision or purpose was that this sort of 12 digit number could be used for authentication identification, and it would be linked to government related subsidies or services to ensure that you're eligible for these and to make sure that there is a broader sort of subset of data that's available on Indian citizens.

What ended up being quite concerning with this initiative, and there have been several sort of court cases that have questioned the constitutionality of this initiative, is that it brings together a lot of this extremely personal sensitive data and stores it in one central repository.

And of course, I think anyone in the privacy world knows that sort of centralizing data in one repository leaves it open to potential for a data breach. Even if this data is encrypted, there are concerns and there have been since I believe, data breaches of this, repository of information, and that's significant if it's such a large subset of people, and if you consider India's population, which is a huge group of people that is been vulnerable to their information being breached by, a number of, a number of folks.

I think the other thing is. Although it was created for identity verification, there are also concerns in terms of the fallibility of these technologies for identity verification. So biometrics like fingerprint scanning or Iris scanning has failed in the past. And it absolutely has failed in the Indian context as well.

When this was used to, for instance The other hand was required. This number was required to register yourself for marriages to even be eligible for availing a sort of like midday school meal, which is something that the government of India provides schools children who go to school.

So for instance, if you were a child and you have to show your authorized certificate, or you have to show. Proof of other identification order to receive a meal, their concerns in which, what that identification or that sort of requirement can do to you can deprive you of services at that point in time, but also enlist you in this sort of

process or system of surveillance in which this data or this sort of set of data can be requested by any entity, whether it's private or public. The issue at the time also that was raised by courts was that this should not be requested by private entities, because then it is unclear to us as individual citizens who is requesting

information on us and why and what the purpose of this will be. So there's been quite a lot of debate on Aadhaar for this reason, both in terms of how it deprives citizens potentially of services, because it was required to be linked right from taxes to, like I said, to avail it, a midday meal, et cetera.

And I think the system was inefficient in itself. But I think if you extend this to a broader sort of outlook on data protection or what data privacy has looked like in the Indian context? I think there's been a concern also for. In terms of what this looks like in terms of surveillance by state actors or non-state actors of the private sector here. And we see also with the way that certain, the data protection bill that's been released that has been tabled, but now is I think going back and is going to be completely redrafted, less significant scope for the government to be exempt from a lot of these clauses

for like national security reasons or for maintaining public order reasons. So we see this sort of time and again, that there are these loopholes where the state creates these exemptions, these blanket exemptions from. What should be a fundamental right and I think, this is significant for us to consider given, like I said the population size that we have, but also the vulnerabilities of the people from whom this data is being collected.

So if it's collected from children, if it's collected from migrant workers who are looking for a certain government schemes or subsidies who may not also have the awareness of their digital rights. They cannot claim them because they don't have an overall overarching regulation. There are quite a few concerns around the accountability of this information, the safety of this information, and the question of process behind a lot of this as well.

So I think that ties into like broader concerns that we're trying to help address or trying to develop frameworks to start thinking through solutions as well.

Eric: In the U S we have Social Security Numbers. I don't know if that's the equivalent, but we take it for granted.

It's baked into the system with its inefficiencies but there's a, it's, there are definitely privacy issues associated with social security numbers and what happens when people get their hands on them. There's been instances of people claiming a tax refunds on the behalf of or benefits on the behalf of deceased people with their, just by getting their social security number and getting some additional personal information.

Suha: I think the concerns extend in the Indian context as well. So identity fraud, this is very much possible and has been the case as well. India, I think also there were concerns that a lot of this data was made open access at one point in time. And so there were many concerns and in the, in also just the development of the program and lack of consultation with, certain civil society groups as well that had these concerns

right at the start. And I think also it's interesting to see, I know we're talking about Aadhaar, but I think it's interesting to see in the Indian context ways in which data is collected for certain surveillance purposes and ways in which data remains to be neglectfully not collected, or we consider data to not exist for certain reasons.

So I think there's sort of two sides of the coin when it comes to data collection and sharing where data can be over collected. And there is this this happens by the private sector most often, but also data can be you can be left invisibilized due to a lack of data.

And we've seen over the course of the pandemic, particularly for vulnerable groups like I mentioned, whether it's migrant workers or farmers where the government throws their hands up and says, we don't have data on this, group, or population of people. And I think the implications of that are also extremely concerning.

And something that we were looking at and starting to think about is how can data be more responsibly collected and shared. And so in, in context of say the pandemic lockdown, a very interesting example of this is that I think at the peak lockdown. So March 20 20 India restricted, all transport.

So public transport, trains, buses, et cetera. What's important to know in an Indian context is that a lot of citizens are traveling as migrants to cities, to bigger cities in search of work. And so when this lockdown was announced, a lot of them wanted to move back home and without transportation,

this is 10 million people actually ended up walking back home. And this was a really long, arduous, really painful journey to witness for the rest of the country and the government, claimed to have no data on migrant workers, let alone on the required sort of mobility information to actually track the returns back home.

And so this gap is really important because it's an infrastructural gap, but it's also a gap in recognition of, their data and sort of digital realities and rights as well. And so we were looking at how. This can be mitigated in some ways by looking at the role of, civil society organizations or the introduction of data intermediaries who already have a lot of data and information on say, migrant workers or on farmers, and likely have a higher duty of care or loyalty towards this group of people and towards protecting this group of people.

And we're looking at how that can extend also to digital rights and data governance and that. So we've seen the possibility of these types of organizations playing a larger role in, in helping represent the sort of digital interests of their beneficiary groups as well. And so that's what we refer to as data stewards in that context.

And I think especially here, when there are concerns around the lack of regulation, there are concerns around existing use of data, existing sharing of data. It's important to identify these sort of intermediary institutions. Trustworthy spaces and build these sort of ecosystems where data can be responsibly shared between different stakeholders by keeping also the interests of the individual or the community in mind.

And that's really what, we're, what we're looking into more, whether it's in migration or healthcare or environmental or climate data.

Eric: And do you think there are certain countries that I guess outside of Europe and GDPR that are leading the way and trying to, taking that sort of data steward, stewardship approach, and how do you ensure that the underrepresented.

are in fact represented.

Suha: Yeah.

So I do think we're seeing some promising results in different pockets of the world. So when I say data stewardship, we really look at it as like an umbrella term. And so within it, we see different models of data stewardship emerge, and this includes data, cooperatives, data, trust, data exchanges.

And we've seen in, I think in the U S there is a data cooperative that actually brings together gig workers who are tied to a platform. So for example, they're working. Uber, they're working with Lyft, they're working with door dash, different delivery workers or gig workers that are tied to a platform that suffer from a lack of data that actually determines their livelihoods, their wages, and an understanding of their role in the broader sense.

Gig economy or platform, economy and what this cooperative or what this data cooperatives aim to do is actually to return that value around data and return that visibility to these gig workers by actually, cooling this data and making it available and more accessible to these workers. And ensuring that they have a little bit more decision-making power around who this might be shared with.

And in the case of monetization, I think these decisions are also. Important to understand and through a cooperative model we've seen, offline cooperatives do this quite well as well. You're able to both vote on and redistribute value in a way that can be quite equitable.

So I think we're seeing sort of the emergence of these data cooperates. Whether it's in the U S we've also seen this in South Africa, in some ways we've seen this in England where we've seen the creation of energy cooperatives that are also trying to monitor energy use and sharing it both within the cooperative itself, perhaps also back to the city, if that's useful.

So we're seeing data cooperatives as a model that has emerged and has been really has given us food for thought. Of how we can have these systems be a little bit more participative and really translate the conversation from what's been really abstract. I think data has been considered an asset.

It's been likened to oil, but really it's such a relational concept that we really want to tie it to individual experiences. So whether it's a gig worker, whether it's a farmer who wants to learn more about their soil, all of this data has been collected and can be a value to individuals. What we've also seen in several countries is a recognition of indigenous data rights and indigenous data sovereignty, which I think is really critical to environmental movements is thinking about

data that's collected on the soil, the land, the atmosphere around us, even if it isn't personally significant or has not been framed to be personally significant can be to indigenous groups and populations across the world. So how do we ensure that it is those communities that are entrusted to do what is right with that data to protect their lands and to ensure that their communities.

Stay safe. And so we've also been looking into principles that have been created in the U S and Canada and Australia and New Zealand that can guide us and create pathways to, to start to think about this a little bit more as well. And I think that's really significant and that's really where our attention should be, is to look to communities and understand really what those priorities are, how we start to translate those into more formal systems.

So we keep this a little bit more. As opposed to this being top-down and really regulation led primary.

Eric: We've had I find the whole concept of a data cooperatives and data trusts. Fascinating. We had Thorsten Ditmarr recently on data cooperatives, but we've also had a podcast on DNA and genetic sequencing for indigenous people in south America.

And, we're also going to have somebody on talk about the possibility for, as you said, like even agricultural cooperatives where you might have farm workers who don't want to necessarily reveal everything that they do, their secret sauce, but to the extent that data can be encrypted and shared and processed, and they can still gain the benefit of sort of a broader base understanding of it versus having to see all the underlying detail of it.

I think that's really where it comes into place. So these concepts of encryption, there's a lot of value to be obtained but all the information doesn't have to be revealed. It only what is required can be revealed. And that's where I think it really makes a big difference, for big state sectors, it's very difficult, right?

Like governments will impose these regulations, but sometimes those who are the least able to comply are the agencies themselves, right? Because they're dealing with antiquated systems, limited budgets, and that kind of thing. So another thing I wanted to touch on India has been growing enormously and its data utilization.

I read a statistic and maybe you can corroborate it: 500 million smartphone phone users with a 35% penetration rate. And that's growing, that's, just, vertically increasing. In, in terms of the number of sheer smartphone users in India, it's just enormous and there's going to be so much

data that can be captured from those smartphones. How can, what are your thoughts on questions like again, we're talking about the individual and consent for, hundreds of millions of people. Are we, can representation be encoded like in smart contract or encryption?

What are your, when do you, cause obviously that's one of the things that you're thinking about in terms of data stewardship, in order to have that data stewardship, it needs also, you need the protections. What are your thoughts on the challenges facing India and the rest of the world?

But India has just such an enormous use case in terms of the sheer volume of smartphone users and their ability to also acquire these devices.

Suha: Yeah. Eric, know this, that's a big question. And I think it's one that we've been chewing on for a little while. And I guess I want to add to the enormity of the situation and the significance a little bit, because it's not just smartphone penetration, not

that volume of data increasing through smartphones, our usage and the metadata that's generated as a result of it. But also we have an incredibly booming, IT sector. And that has also seen, proliferation of different technologies, whether it's IOT, whether it's, there's various startups that have emerged.

I'm sitting in the startup capital in some senses of India. And we've seen, half a dozen unicorn startups that are, have emerged that have very data-driven business models and these business models also tend to be, they there, their bedrock of their foundation is a collection of massive amounts of data across different sectors.

So I think, just speaking to the volume and the enormity of data, and like you said, also the concerns around a significant group or population in India that is now going online and increasingly navigating this digital space. I think the concerns that we're seeing in some ways is twofold, right?

So there are questions around an understanding of data literacy, data rights, and that's coupled with technical literacy, which is still, we're still remains to be a challenge in India. And we see that in, in order to. In order to address that. And we also need to look to the existing human architectures on grounds, the existing community work that brings people together.

So for example, I'll give you an example when COVID times, when you have to register for a vaccine, you had to register on a portal called Cohen. And this was an online portal that the government created. You had to be able to verify your identity through your phone and you would receive a pin on your phone.

And that was the way in which you could actually register for a vaccination now, considering India's population. Although we have, mobile penetration, it's also gendered, right? So if you look at a family, the woman in the family may not have access to a phone necessarily. It might be the male in the family that has access to a phone.

There's also a concern about, those who are at the last mile, who don't have access to these devices, don't have access to this technology. And so looking at the human architectures around it, how can we look to existing community-based organizations, grassroots organizations to help fill in this gap in some ways.

Help make the capacity available to both understand the technology and provide linkages that are offline as well in terms of the delivery and access component of it. So I think that's the offline side of things. I think on the online side of things you will have to come up with better solutions.

You mentioned consent. And I think that's one dimension to the concerns we're seeing the data economy. I think consent is one approach to participating more, more broadly. And I think even consent in the way that it's imagined in other populations and other parts of the world has also failed.

We've seen how, noticing the consent mechanisms in the west still don't provide individuals who can read, write access online systems with an understanding of what's happening to their data or why. So I think even considering that the issue is consent related, ignores the vast other components and the kind of engagements and structural sort of ways in which data is collected.

So passively, we don't know about it. We don't know about its value. So I think going back to the solutions around. I think it has to be a set of solutions. And we look at data stewardship is one piece of the puzzle. And I think that one piece of the puzzle even has to be looked at from two dimensions, right?

It has to be supportive top-down so through more supportive and more responsive policy that really puts the citizen at the center of the equation a little bit more and recognizes that there is community value to be had from this data. And I think one of the contentions there has been,

like I said, we have a huge IT sector and there are concerns that, this legislation can actually threaten the ease of doing business, threaten the growing of this industry as well. So that's one side of. I think the other is the bottom up interactions. So as I was mentioning, there's a huge community

people who are going to be going online, whose data is already being collected, how do we involve them in these conversations start understanding what data means to them, how it's valued and have them be part of the conversation. So whether it's through data cooperatives, whether it's through other modes of engagement, really sensing the pulse of saying, okay, this is valuable.

That you can use, and you can determine how it's used. And so I think kind of building those structures from the ground up will require, piloting out these systems of data stewardship a little bit more also, highlighting and maybe raising this issue for funders who are now looking at digital technologies, the development of AI systems as well.

This becomes a significant part. Data governance has to be considered in this sort of exploration for new technologies and the applications of these technologies. So I don't think there's one easy answer. Just seeing how it's installed, whether it's in the Indian context or globally. I do think there will be a significant role to play from public institutions, but also from private institutions.

Possess a significant amount of data as well. And making this available to citizens or having greater transparency around its collection will be one part of our sort of understanding of how we start to build structures around it as well.

Eric: What are the risks of weaponizing data for targeted communities?

Not so much where a government entity. Doesn't take an action or doesn't account for these communities, but where there is a group that is affirmatively taking an action to use the data and targeting these communities, due to bad data stewardship.

Suha: Yeah. I think we've seen a number of examples of.

Specifically, really personal information being able to locate a certain group of people or put together patterns of where this potential group of people could be from what their religious backgrounds are, what their sexual orientations are. I think most recently we've seen that the weaponization of data can really extend to a, quite a broad group of people.

So I was talking about fem tech earlier about a lot of applications that are collecting data on your fertility, on your mental health. And I think a big concern that you've actually seen in the U S and that can be a global example for us and something that we should take notice of, is how the collection

fertility data that has in the past also been shared with platforms can be used to actually, target groups of people that are going to say reproductive health centers family planning centers. Both identify where they are in their cycles, what they're Sort of interventions are that they're choosing to seek and how those can be, how they can be targeted on that basis.

And that's on the basis of whether it's location data, whether it's fertility data, this is sensitive, very personal health data, and the information that's shared, not only with private sector entities. But that, can be shared with, a number of groups with nefarious intentions as well. So I think when it comes to things like reproductive health, we have to consider, the gender dimensions of a lot of this data and a lot of this information.

We've seen how location information in the past from dating applications has been used to actually identify, I think there was a pastor, for example, which was identified as going to, a gay bar and then he was outed by the community. And I think, these are the concerns from geolocation data.

And I think part of what we're looking at in terms of stewardship of information is that when you come down to, looking at safeguards to protect this information, we assume that things. Encryptions are there. Okay. And as long as data is being shared with one entity that you know of, it's going to be fine, but I think studies have shown that, even location data when removed of all of its personal identifiers hat still has risks of being there are risks of re identification possible.

If you aggregate this data again, Other publicly available data sets. And so I think their visits are always going to remain and I think we'll have to be extremely vigilant about ways in which this data is collected. I think we're seeing some progress in terms of having this data collected at the edge, so that there's a little bit more control of this data is collected on your device.

It remains on your device, and it's only used for certain, very purpose restricted measures or, what you've consented to. But I think it's also up to us as individuals to ensure that we're pushing for more sort of data minimization, and the way that we're thinking about this.

So if you're, logging into an application and they're asking you for location data, You really don't need to give them for that particular service. In some ways it's also about us being a little bit more vigilant about how we engage online in some ways too. And, considering your mind behaviors a little bit more as well and restrict location usage.

So I think there's an interpersonal solution to that at some point. We don't have a lot of control around this so far. Like I said, systems are still I'm not a hundred percent in terms of protecting these forms of data and this can be used in terms of weaponization really across the board.

I think it's concerning to think about. You know how especially vulnerable groups can be particularly at risk of this data being made available to even, state entities. So I think we saw in Afghanistan most recently that a lot of the data that, belonged to civil society organizations, if that, went into the hands of the Afghanistan government now that puts a whole swath of women at risk.

It puts a whole squad of children and other vulnerable groups at risk as well. So I think. This requires also inter international institutions to take a really hard look at ways in which they are collecting data as well, even if it's at a proxy level to ensure that there are there are both indications of what the experiences are like people who are from marginalized communities.

So we are, and should be collecting gender dis-aggregated data or data that relates to vulnerable communities. But if we are doing so, what are the mechanisms with which we consider the safeguards, but also accountability and transparency around that data as well. And making sure that we have full visibility of that life cycle of that data as well.

So yeah, that's what I'll say. I don't think again, I don't think there's an easy solution to this just yet. But I think we have to keep pushing.

Eric: Before we break, what are some of the initiatives that Aapti is working on now that you're particularly involved in maybe particularly passionate about, specific example.

Suha: Sure. So I think as I mentioned at the start, our work has been, has revolved around this data stewardship landscape and our methodology has been really case study driven. So we've been speaking to organizations across the world who are governing and collecting data and more new and innovative ways.

We were looking at ways in which communities can better engage with data and participate in these systems. And now I think, considering what we've learned, and we want to make a set of resources available for those who are actually building out stewards or building out institutions and help support them in that effort, and understand how they can speak to their audiences a little bit more about these questions.

What we're also focusing on now which is quite interesting, is looking at the broader ecosystem of how data can be shared among these different intermediaries. What needs to happen? What's the foundation required really for say a data cooperative to speak to a data trust, to speak to a data exchange, for instance or say a public

government repository of information, where do we fit into the broader sort of like patchwork all of these different entities and how they relate to one another. And we're doing so with a specific focus on the environment and sustainability, because we see a lot of information and data that requires to be in coalesced and aggregated from multiple different stakeholders.

So one really interesting thing. Working on right now is what, speaking to a network that is bringing together a variety of stakeholders, which includes, researchers and academics include civil society, organizations who are working with indigenous people. And their whole aim is to say, how can we bring together really important data and make sure that it's held in this repository where it's safe, it's made available, it's made accessible, it's interoperable, it can be shared with other entities and really going through the dynamics of what that looks like. And also considering, environment and the focus on environmental data and other really interesting project that we're starting to do a little bit of work on is around air pollution data, which in India is, a significant concern as well.

We ha we are home to, I think, many of the world's most populated, sorry, populated, but rather polluted cities. And we have a dearth of. Data from the public sector on air quality. And so it really comes down to the private sector and civil society organizations to both collect that data and make it available.

And there are efforts now to understand how communities through citizen science efforts a part of that can be. From installing sensors in their homes, being able to better track, what the air quality metrics are like and having that as a foundation to then lobby with their governments, for interventions to really mitigate the risks of a lot of this.

So I think we're seeing some really interesting movement in that direction, around the environment. Similarly, around healthcare, we've seen with the pandemic, the necessity to have this information at our fingertips, but also to do it in a way that respects the sort of dignity of patients of their rights and considering the sensitivity of this information as well.

And then lastly, smart cities and mobility, we were talking about the concerns of location, data being shared. And I think part of the research I did a little bit earlier was looking at how this data, this location data can actually be quite significant in the way that we understand, say, how women move around cities and how transportation can be a little.

Responsive in the way that we design it, how our cities can be made more habitable and more gender responsive based on our understandings of, mobility trajectories how we can understand the implication of things like lockdowns or things like That or, enforcements that have been put in place with the pandemic.

I think location and mobility data has been extremely influential important for us to be able to share at a sort of hyper-local city level, but also with our, national governments and also internationally. So I think we've also been looking at sort of those instances and speaking to in some ways, multiple stakeholders who are involved and invested in these questions.

And I think that's been really exciting is that we get a really diverse set of experiences, and an understanding of how different folks are thinking about this data and thinking about the sharing of this data, whether it's a government agency creating a data exchange for mobility data. Whether it's a civil society group working with, indigenous communities and looking to preserve, digital rights, whether it is a broader network of people that's trying to coalesce multiple different stakeholders.

So I think all of these perspectives are super, super interesting, and we're hoping to dive into these questions with in, in a little bit more depth as we go along and better understand, like I said, from the people what this can look like and doing this through working groups doing this, hopefully through the creation of resources that can be actionable and can be something that communities or

businesses are stewards that are evolving, can actually use and implement on ground as well.

Eric: Great. It sounds like you got your work cut out for you.

Suha: That's lots of work that if you're interested in, in, diving into these questions with us there's a lot for us to continue to unpack, I think.

Eric: Yeah. And so where can people go to find out more about Aapti, and yourself and the work you're doing.

Suha: Yeah.

So the work we're doing at the Aapti Institute, you can go to up the Aaptiinstitute.com to learn more about our work. And more specifically the work around data stewardship. You can visit the data economy lab where because we are a public research Institute, any of the research that we publish either with partners or otherwise.

It's made public and accessible to see, and we have a set of tools and articles and resources that we continue to build up. And we'd love to hear from you and your community of listeners as well to see if there's anything that like to partner with us or explore questions together. I think there's, like I said, Eric, lots for us to figure out and I don't have all the answers, but there's stuff that we can grow and develop together, I'm sure.

Eric: Great. Thanks so much for coming onto the podcast.

Thank you so much Eric, this was great.