Workshop on 'Privacy after Big Data'

Held on Nov 12, 2016

Venue: CSDS, New Delhi

Session 1: Introduction

A: Big Data, as a term, sucks. Lets us begin with examining the limitations of this terminology. The terms ‘big data’ is an industry term and immediately evokes notions of other ‘big’ industries – big pharma, big oil, big tobacco. One of the one hand, the terms implies is that big data is about size of datasets, on the other hand it indicates that big data is about the size of the industry emerging around data. However, the phenomenon, unfortunately described as ‘big data’ is about much more. It is a new way of thinking about and working with data. Rob Kitchin has argued that Big Data is qualitatively different from traditional, small data because of its ability of accommodate unstructured and diverse datasets.

The 3Vs definition has also been shown to be inadequate. It is highly unlikely that any data-sets satisfy all of the above characteristics. In fact, a review by Kitchin and others of 26 different datasets generally understood as Big Data revealed not all of them even satisfied the three V’s of high volume, velocity and variety. The obsession with the V words is best captured by Uprichard who several other v-words: ‘versatility, volatility, virtuosity, vitality, visionary, vigour, viability, vibrancy... virility... valueless, vampire-like, venomous, vulgar, violating and very violent.’ On similar lines, Lupton has suggested dropping v-words to adopt p-words to describe Big Data, detailing: portentous, perverse, personal, productive, partial, practices, predictive, political, provocative, privacy, polyvalent, polymorphous and playful. What is important to remember is that these words, while useful entry points into understanding big data, do not actually describe effectively the phenomenon of big data.

When we see phenomena such as database state enabled by UID, network infrastructure under Smart Cities Mission, cradle to grave identity under Digital India and transaction generated information generated by digital payments in a cashless

economy, these are all key examples of big data even if they may not satisfy the 3Vs definition.

With that we begin today's discussion on big data and privacy. My purpose was to break down the term 'big data' and prevent it from creating a hurdle in critical discussion and research. B will take it from here.

B: Thank you. Data has to be generated, data changes, you have to collect data, organize it or create it from scratch, text need to be written, photograph needs to be taken, video and audio need to be recorded or they need to be digitized for modern day existing media. Now we live in the times when a lot of data is generated automatically through machines but even then there is a certain association of the design of your computing system and the kind of data it generates, it just doesn't fall from the sky despite. Iza Gittleman and Jeffrey Cobb and others have argued that big data is an oxymoron, it tends to be imagined as data to exist and function as such and the imagination, entails and interpretive base.

Moving on which brings me to another propagation is that we need to think through the material complexity and specificity of database systems. Last 30 plus years all our systems have been running on something called Relational Database Management Systems. A lot of data exchange – changing today when we move to big data systems, normal DB, Apache and so on. So, we need to think that where does data analytic gets its power of generalization and prediction? How is it that a certain set of technologies is agnostic to whether it is being implemented in a health sector or education sector or software industry and so on where are those being generated and how? What are the differences between statistical analysis of large data sets versus big data and what were the epistemic shifts leading to the data revolution and when and how did the web change from a messy dump of pages to a searchable network, right? And going back from the '90s – early '90s the day it went the – the dissolution went in the retail sector in US that you have all these databases, perfect storage but how do we query data? So, the problem with which most of the big data fundamental debates on retail started had nothing to do with the kind of importance as we see now. It was about how do I retrieve data from these databases and how do I make correlations? And how dependent are these systems on cost of computing and infrastructure seamlessness?

Moving on to another point which we need to – another field which we need to think about very deeply is that history of statistics in India – statistics as you know it goes as long as the history of statecraft and nation states and the social data ecosystem in India which has been around since at least the modern social data ecosystem in India has been around since the first census by the East India company in 1868 and much before that as well as different princely states have their own formats of record keeping and making numbers of our populations. One particular reference which I'd would like to give here is of PC Mahalanobis who since the 1930s leading up to '50s was a key architect of the statistical infrastructures the Indian states has today. And a defining feature of the rise of statistics at that time was the evolution of the sample survey methodology by Mahalanobis. His idea of data was explicitly defined by what was considered feasible to collect by the field staff with low literacy levels over large populations and area sizes with minimum expenses. So, these problems have remediated over time but are still pretty much part of the conversations we need to have on big data.

The other set of issues, which we feel are pertinent today to discuss, is the idea of surveillance. We have moved from the overwhelming concern around surveillance to that of source valance where increasingly citizens are recording information using technology that has become affordable and easily available. What we have begun to see is the era of the citizen using sting operations, group of people who decide to monitor social media to control communal tensions, citizen using drones etcetera. New Media scholars have began to characterize new modes of control as surveillance, raising issues of due process or accountability more than totalitarianism. Tom Boellstorff an anthropologist of computing says that, he master minded for big data and surveillance as, is the confession rather than even octagon where, rather than being subject to a purely invasive gaze, people willingly confess their data.

And the last major issue which I need to touch upon here is the blurring of public and private. The 19th century social theory model of this is public, this is private is up in the air now. With the increasing use of Internet enabled mobile phones and the cultures of forwarding, easy circulation of media and inter media exchange, there is a challenge to think about traditional notions of the distinction between public and private. Many of us are familiar with the JNU episode and what happened when material that was posted on Facebook led to quite a circulation and meanings transformed and it

acquired its own publics and velocities and there were several debates around the privacy settings as well. But what does it mean to say for instance, that the test of incitement to violence in public order cases is based on the proximity to violence when potentially every act of speech is capable of being recorded and transmitted on WhatsApp with potentially massive audiences? What is the status of public data on social media sites? Researchers by the way have been debating whether you can cite to it just because it's public or do you need the permission of the person who put it out there. So, these are not clear cut issues.

Just because data is publicly accessible it does not mean that the content was meant for everyone. How does this impact the ethics of research and data collection and yeah and this in turn is playing to the emerging debates around right to be forgotten where increasingly there is a ethical and legal scrutiny over the digital traces that we leave and the control we have over our data. There are many more issues to be retouched upon but we have very little time and I think we should start with the first session.

Session 2: From Privacy Bill(s) to 'Habeas Data'

A: We move on to the next session. So, if you can take your seats then we can begin.

C: Let's do some privacy. So, I – I'd actually told S that my interest at this point is not just on privacy and privacy bills and privacy laws but on why a government would go to a court and say that the people of this country don't have a fundamental right to privacy? Why are they saying it and why are they saying it now? And why are they saying it, in the case in which they said it? Because at the same time that they went to court and said that, you know, in the UID matter when they went and said that we do not have a fundamental right to privacy, they were down the corridor in another case in the defamation case, they were saying that, privacy is a fundamental right of these – of the citizens of this country and we have to protect it and therefore we need to retain a criminal law on deflation, because that's the only way the state can intervene in protecting people's privacy. So, also interesting that when the court gave the decision ultimately the court gave the decision in the deflation matter, they would not, you know, they decided to skirt the issue of privacy and went on something which is completely – which doesn't exist in a jury's prudence and which is much more complex and which I don't think was addressed at all saying that there is a fundamental right to reputation. And that's a whole other game and it has, actually it's

unexplored nobody has any idea what that means and what that does to what we can say, you know, what we cannot say whatever.

So, not only did the government take two positions in two different cases this court too was unwilling in the case where privacy was being promoted as a right to adopt it. So, there is something happening not in the state of Denmark but in state of India which is complex. And I don't think we know there are multiple promptings and there are – what gives me the confidence to make hypothesis is that from at least 2009, when the UID project started almost every hypothesis we've made has turned out to be valid and unfortunately true. So, therefore I'm not advancing this just as a hypothesis but also because of many things that have been said. So, I just thought that I'll share some of the things that I am noticing and I'm sure many – I know each of us will be noticing various kinds of things.

What kind of things are being said to us about why we need to give up on privacy, from the past 7 years, what have we been told? One we have been told it's a question of convenience. Convenience as we know is something that we choose. We may decide that we do not want a certain kind of convenience but we're being told that convenience will be public policy and therefore anything that will be more convenient and they don't say convenient to whom but it's about convenience. So, convenience can prompt coercion that you have to be – you have to make things more convenient to yourself. So if it makes sense and I want to hark back to this, you know, when they JAM now which is where they have us but when it started they started with saying that we have, you know, and Nilekani is being the spokesperson throughout. So, it's his language that we'll hear resonating all the time. He said at one point that, in this country, 'Roti, Kapda aur Makan', that is you know, food, clothing and shelter are now passé and it is now what everybody wants and what is really in is UID number, bank account number and mobile number and if you – and that's what's become JAM. So, you know, all these acronyms that are being created and the slogans are being raised are actually going back to something that has been like Nilekani's own right hand man Pramod Verma says in one of those videos, he says that it's been evangelized to us. So, it's interesting that we are not being given information about anything and we are not being, you know, for instance no feasibility studies are given, no information on the actual processes that are being put in are given, no idea of costs are being given to us,

no ideas of liability are being propounded at all but we are being evangelized the change of systems.

I think it's also very important to investigate the language that's emerging now and that language of disruption is a very interesting one and I think the way in which disruption is being promoted is that, you know, there are many, many moribund systems around us and they need to be cast out. So, you have to disrupt that with new, you know, new systems that are coming in. Now what we are finding underground and which is what we have been saying forever is that, disruption will certainly happen but disruption happens by disrupting and destroying existing systems with the intention that you cannot return to it and therefore you have to transfer yourself on to some other system. Whether that system is complete whether it can actually perform what it is supposed to do that's not important. What is important is that you have to destroy this otherwise that has no market. And the kind of disruption that we are looking in the banking sector but interestingly I just want to mention one thing that we see all around us now. The PDS system, the Public Distribution System, where they say that the idea of disruption there has been by using technologies which they are not looking to use anywhere else on people on whom those technologies will never work. So, you have biometric technologies for manual workers who are the basic class of people who go to, you know, who go to collect rations in a public distribution system, in a fair price shop, and they can't authenticate themselves. And then you keep conjuring up figures which have no meaning at all.

So you say we have saved 50% of what we were spending on this – we have saved 30,000 crores which have no meaning at all because you have basically pushed people off the system because their system – you know, it doesn't work and then you say we have saved it and everybody else is a ghost and a fraud. So, we of course have a whole spirited culture evolving with number of ghosts coming up in different places and ghost suddenly remerging as live people. There are multiple stories that we have in this. And the pension system in Rajasthan, in Jharkhand and the intricacies of that of course we don't know at all. So, the private is not only about, you know, privacy is not only about hiding something from the other or not allowing people to peer into you but also not to be misrepresented for who you are. And the idea that you don't exist is as much a violation of privacy as saying that you should exist only in certain forms

where I can view you and see you and this is happening a lot. In introduction I should say that I work in law and poverty so it's been, that aspect of it has been of particular importance.

The second thing is that, you know, the next kind of thing that's emerging where they say that India is a data – the first thing of course was UID they said nowhere in the country – nowhere in the world. So, we have become a nowhere in world country where we have to do things which hasn't happened anywhere else in the world. So, nowhere in the world is there such a large biometric database. Nowhere in the world do we have a database that will allow all kinds of systems to be built on it. Nowhere in the world I'm sure you have our identities becoming platforms on which multiple things get built. Nowhere in the world is going to be as data rich as we are going to be, we are a data poor country and we are going to become a data rich country. So, I just want to quote Nilekani on this he says, "Finally as India goes from being data poor to data rich in the next two to three years, the electronic consent layer of the India stack will enable consumers in business to harness the power of their own data to get fast, convenient and affordable credit. Such a use of digital footprints will bring millions of consumers and small businesses who are in the informal sector to join the formal economy to avail affordable and reliable credit. And as data becomes the new currency, financial institutions will be willing to forgo transaction fees to get rich digital information on their customers. The elimination of these fees will further accelerate the move to a cashless economy as merchant payments will also become digital."

So, the idea that you have to give information about it – he was talking about confession, it's not confession at all lot of this is coercion. And if you do not give that information you do not get the service and these are not some services which are esoteric services, they are basic services like food, like getting access to the income that you have earned through your work that will now be dependent upon your being willing to give up information about yourself. And there is since we don't have any privacy regulation, no norms, no nothing it can be any kind of information that they ask and you damn will give it or else you are out of it. So, you can earn, the money will be put in to your account but till you give all the information that's being asked for you, you can't – you can't use your own money, I don't what cashless means beyond that.

Then there is a 2010 document, which is a national data sharing and accessibility policy of 2012 and they have, you know, this is the I think, I don't know, we should check this out but I think this is the first time that the government has said that they own the property that, you know, own the data that we give to them. This idea of ownership hasn't existed, government owning anything did not exist in this country, government is a custodian. So, from being a custodian to becoming an owner and to asserting that ownership, has just taken a document that's all. So, in that document they say for instance, 'legal framework data will remain the property of the agency, department, ministry, entity which collected them and recite in their IT enabled facility for sharing and providing access. Access to data under this policy will not be in violation of any acts and rules of the government of India in force. Legal framework of this policy will be aligned with various acts and laws whatever. Pricing of data if any, would be decided by the data owners as per the government policies. All ministries, departments will upload the pricing policy of the data under registered and restricted access within three months'.

A couple of days ago, two three days ago there was a newspaper report which said that, you know which, it was titled, 'commercial acts will soon be able to strike open data gold'. And they say that that the government generates – actually it starts like this, 'center will soon notify a policy that will allow apps and services to be created for commercial purposes using over 42000 databases. This will remove the restriction on their use solely for academic purposes'. The open government data platform publishes data sets from various ministries and this additional secretary to the ministry of information technology says, "The government generates so much data a lot of people can use them. For example, census data are used by academics, companies, students and politicians. Data are a very important source", and they go, you should read the full report. 'Earlier we permitted their use only for academic or government purposes, we recently took a decision completely un-discussed, un-debated, un-informed of the – I mean the public not being informed, we recently took a decision to allow people to create value added services for commercial purposes'. And they said, 'the policy will be notified soon it will allow anyone private, government, academia or start-up to offer services. The government will not charge for data but the provider may price the services'. So, we give – we pay twice over in a sense, we give the data to the government, the government then decides which of that data and you as a person has no choice in deciding whether, you know, they don't

even ask you and there isn't even a public debate on this. They decide what they will reveal, how they will reveal it, who they will reveal it to and anyone who wants can make money out of this.

Now this is not at all a surprise and this is part of a pattern and I think we should go up to the tag up report to see what the idea of privatizing of government data was. I think one of the ways in which this got frustrated was when the UIDAI intended to be a private company and as you can see from the tag up report and all of us together frustrated them so they are having their own revenge. This is their way of saying, "okay it didn't become private data but we have multiple ways of getting access to it and doing what we want with it." And that's why Section-57 of the AADHAAR Act is a very important provision, this – that was their revenge. They said, you know, "you – if it's not mine I will make it mine in multiple ways". I think we need to look at the kind of things that are emerging from within that domain, that Section-57 area because they've started with the labor market and it's really scary the kind of companies that are coming up and what they are saying they are going to do. There are three companies that I have noticed. If there are more we should share that information on them, there is TrustID, there is OnGrid and there is BetterPlace and these companies have, you know, advertised themselves as being AADHAAR enabled and they say that they will get immediate, you know, you just go to them with whatever information and it's completely, you know, the idea of consent I've never heard a more perverse use of the idea of consent as in every system today, it's completely outrageous today.

So, I think cleverly Mr. Nilekani is an intelligent man, so he has kind of moved from saying consent to saying consent layer. So, it's maybe another kind of hen I don't know what it lays but, you know. So, the idea but the idea of consent has vanished. So, these guys say that they will immediately authenticate whether the person is the person who you are checking up about and then they will scour all the public databases that are available to create a profile of the person and then they will inform the person who wants to employ them, you know. So, it's a very clear class kind of divide in this. And then you can go back to them as an employer and tell them, you know, this guy was good for this reason and not good for that and, you know, he drinks or he has, you know, he loves women or whatever and then that will decide whether you want to bring them back from Bihar for your next job in some place. So, they say, you know, people don't need to move we'll tell you, when we want you to

come because you're not going to get jobs unless you are in this system. So, these are systems that are being created. Mr. Nilekani has been talking saying, he's been again evangelizing saying get on board quickly because we're creating monopolies it's a WhatsApp moment, if you get in at the ground floor you are there if not you lose out so there is a lot of push for this.

So, the second one that they're doing is a Fintech company and surprisingly Mr. Nilekani has himself signed on to being the promoter of a Fintech company which I did not expect would be so open and would be so quickly because he's plainly, you know, the UIDAI people have stepped off, they formed India's stack. They are now creating products which they take back to the UIDAI and they donate it to the UIDAI so that they can say we don't have any money interest in this. And then that's going to be used for things like this, the Fintech companies now. And there I think we need to investigate everyone of this, cashless we need to understand but I mean that's the most absurd of the propositions. But they also have paperless and we all know that in addressing corruption one of the most important things for us has been the paper trail and that's because we too can look for the paper trail whereas when it's a digital trail we neither control it nor can we reach it.

And the third which is presence-less and this is really significant. What they are basically saying, you want privacy I'll give you privacy, you don't exist. You don't need to be there. I don't need to see you, you won't see me. And this idea of who, you know, you don't even know who you're talking to, who's talking to you and who you are addressing and where to go if things go wrong or even if things don't go wrong and then on top of that they say you have what they call a consent layer. And there are very interesting YouTube lecture, talks on all of this, where for instance, In the chart giving us run down of how in eight minutes they will give a loan. And they say, you just send in and then – and everyone of this has UID person in it. So, e-sign is singed on to by Ram Sewak Sharma who's now TRAI Chairman but who was in his earlier avatar, the mission director of UIDAI who went through the department of information technology into TRAI. So, it's all loyalty branded self interest which is promoting this and I think there is no running away from it. So, they have e-sign and then they have e-KYC and I think it's significant, the extent to which we've all become KYCs. We are all just customers, we are losing citizenship and we are not even noticing what that means.

Citizens are entitled to privacy. Customers are being told, you are not. And since we've all been converted into customers, the idea of privacy is just dropped off. You want the service you give me the information I want. The two things that have dropped off the map, one is the national population register, I think we shouldn't forget that it exists and what it said. There is one clause in the manual for those who go to collect data where they say, it's not enough for you to find out to get the names and addresses, whatever. But reminding you of Edwin Black's book, they say here that you need to ask them their relationship to the householder and if they say uncle, nephew, whatever not enough, find out brother's daughter, sister's son whatever. Every meaning, all the blood lines have to be clearly demarcated in this. So, I think we need to remember that that exists. And there is another one which is, I mean there are lots but other area that's going to impact us in terms of privacy and in terms of who we are is the collection of statistics act. It was the first time, actually the second time after the citizenship rules, where they said they would penalize us and the first time that they said they might penalize us even with imprisonment if we refuse to part with information and the data that they may collect may be about anything at all and they don't have to explain why. So, this is the scenario in which I am thinking that they've decided that the right to privacy simply does not exist in practice but that it has to be legally destroyed.

D: Thank you, so, the first two two speakers spoke basically about big data and then B spoke about privacy I'm going to try and bit up and talk about the intersection of big data and privacy and just briefly outline the privacy issues that big data throws up just so that we're all on the same page. We were hoping to send out a background paper but that couldn't happen. But I'll just briefly list out these issues and we want to start a conversation about the concept of Habeas data and see if that is something that we can use to address at least some of the issues that arise with big data and privacy.

So, talking about the major privacy issues of big data, the first one is obviously consent. Now, consent in recent times has come under a lot of criticism in the entire privacy paradigm because a lot of consent forms are really long, verbose, people don't understand them, there is no negotiation, you can't really modify them, all of that. but most of these problems are problems with consent per se and they come out of big data. The problem with consent in big data actually comes from the collection limitation or usage limitation which is, when data has been collected, assuming

consent has been taken when it was collected for a particular purpose what big data allows you to do is, at some later point of time, use that data for another purpose. And that is where the value of big data lies. And that is exactly where the problem with consent also lies because at that time if you have an existing data set which was collected for purpose A, you want to use it for purpose B. Even if you want to take the consent of the people involved, you cannot take the consent of the data subjects because there is just way too many, it may not be practically possible. So, consent is an issue we have to deal with when it comes to big data.

The second issue is data anonymization. Now, data anonymization in the traditional privacy paradigm was used as a very essential tool for privacy protection when it came to data collection. However recently trends in big data have shown that data anonymization may not be enough anymore because you can use publically available databases to connect and identify particular individuals. There are number of examples of that, Netflix data, AOL data etcetera. The third thing is retention limitation. Now, in regular privacy juries prudence we have always assumed that data should only be retained for as long as it is necessary. In fact even the law recognizes that. But big data comes in and then wants to change that. I mean for big data to be successful, to be commercially viable, it has to change that because the fundamental basis with big data is that you want to keep as much data with you as possible because you never know what use it will come to at a later point of time. So, therein lies another inherent contradiction between privacy and big data which also needs to be addressed. The last one that I wanted to talk about is something that C also mentioned which is that these data sets actually have a commercial value but it is generated by the data subjects. Now, this was a point which I think came about in our last workshop at CIS, should the data subjects also be entitled to a part of that commercial value which the data set generates? And if the answer is yes, then how would that be actualized? So, these are the main privacy issues that I wanted to bring about with big data.

The other thing I wanted to talk about is the Latin American concept called Habeas data. I wanted to see if this is something, I mean, I just wanted to start a conversation here and see if this is possibly something we can explore which would address some of the problems with privacy in big data. Now, Habeas data is basically a writ that allows you to go to court, in number of countries it is a constitutional right. It allows you to go

to court and ask the government to give you any data they have on you in any data set and the purpose for which that data is to be used. Now this is a constitutional right in Brazil, in Argentina, Columbia, Venezuela. In Asian countries Philippines has recognized this right. It basically came about in a very specific context where government surveillance used to lead to a lot of government sponsored violence against the citizens. And therefore people wanted to know what information the government has on them as a protection for them.

So, the essential features of Habeas data according to me and – here, this is just from my personal readings on this is that it is the right of every individual – so basically there are four things that Habeas data gives us. It's the right for every individual to ask for his or her information in any data registry and the purpose or use to which that data is being put. The right is available only against the government or private entities having a public character. In one or two jurisdictions this right maybe available against private entities, purely private entities as well but usually it's only available against public entities. Thirdly, it also gives you the right to access and correct wrong information. So, access and correct is also a right we talk about quite often when we talk about privacy. And Habeas data gives you that right as well. And lastly it is a right available to you by approaching only one particular forum. So, you don't have to go to each department and ask them if they maintain a database on you. You go to one particular judicial forum and you ask for the data and all of that data has to be given to you.

I had also sort of analyzed Indian law and what we realized was that some of these rights at least in India we do have under the RTI act. You can under the RTI act approach the government and get information on whatever data they have on you as long as it doesn't under one of the exceptions under the RTI act. And again, the RTI act also, this right is available against public, against the government as well as against public entities which have a governmental character. What we do not have under the RTI act, which we would have under Habeas data, is access, is the right to access, is the right to correct wrong information. And a big problem we would have under the RTI act is that you have to approach different forums. There is no approach to a single forum where you can approach the Supreme Court or any high court and ask for all of this information. I think Habeas data might be useful because a lot of problems and a lot of anxiety at least amongst people when we talk about privacy and big data comes

from the fact that they don't know what use their data is being put to. And at least that one aspect is something that a writ like Habeas data can address. Because at least you know what data exists and what use it's being put to. So, that's it, that is just the thing to talk about.

A: We have half an hour for discussions, so, questions.

Q: So, my question is for both of you. I just wanted to ask, what D was saying now about Habeas data is something very clearly about how citizens approach the government and the commercialization of data is where customer – you are making a customer out of the citizen. So, is this something which will strengthen the citizen because it's a constitutional right you are saying in some places? And what did this come up as a response? You're saying it's about violence but are there other invisible forms of all this violence which was going on to make, you know, people into spirits and people into ghosts? So, I think this is the question.

D: So, so far is it empowers the citizen to get information from the government. It's definitely going to be very empowering if we can actually get this right in India. Secondly, we shouldn't – at least this is my personal opinion that we shouldn't really harp too much on the background in which it originated. It's a right which may have originated in a particular background but that doesn't necessarily mean that it cannot be applied in other places. Which is why I think, when it originated in Brazil and Columbia in the '90s big data wasn't really an issue. But it is something that we, it's a tool that we could look at to address issues such as big data.

C: Largely that's true but I just want to put in a few caveats in this, one is, in the RTI the exceptions allows the state to take away many of the things that – so they'll say it's a national security. Now national security you can't question. It's like, that's it. So, there are multiple and there are agencies which are outside it. So, if NATGRID worked at getting itself outside, so they are outside of it. So, that's one. Second thing is that, if you look at the regulations in the UID act, they've said that there is confidentiality of the contract between, you know. So, they introduce confidentiality through laws which actually militates against openness and they are just putting it in. So, there's nothing confidential about us that they cannot know but there are things confidential which are protected about – so you can't get information out of it. The third I think one interesting that's happened with the, again with the UID is that, biometrics for

instance. Our own biometric data we are not allowed to see because they said that, it's such sacrosanct data that they will not give it, they will not allow it to be used in the national interest, they will not be allowed to use it if a court orders it in relation to a criminal investigation or whatever and you can't see it yourself. I mean that's like – and they've said that this is a privacy interest. They're protecting you from yourself. So, I think there are many ways in which we are being already shut off from information on this. And when it is private companies which are being generated to use all of this, they don't have to give it, they don't even come within the RTI.

Q: Would there be any way to analyze how the response such as what B was just saying on the issue of, your biometrics is not to be known to you and your data is also held with the government, doesn't come under RTI very easily. It's prevented through confidentiality contracts. Is there any way to analyze whether this is actually response to something like where a constitutional right now exists? So, is this a protection for commercial, corporate, profit oriented interests, very clearly saying that we don't want to come up with, we don't want to come out with what we are actually going to do with all this data. So, I think we should actually maybe tag this a little future.

C: Yeah.

Q: So, two questions actually to both of you. First is I think increasingly we are seeing privatization of public interests. And I think that is precisely what is raising a lot of these issues or creating an urgency in a lot of these issues. So, in terms of the exercise of – actually that leads to my second question. The second question is basically that if you look at the notion of KYC for almost everything that we do, now they have the concept of extended KYC. And the extended KYC actually is something where you give rights to transfer your data to unspecified and unknown entities in perpetuity. So, - and you have no way to opt out. You either opt out of Access to the services or you submit so, I think this raises a whole issue in terms of you know, whether such content contracts are even binding and legal and should they actually, have they been challenged or should they be challenged in any place, anywhere across the world?

D: Okay the second part is something I can look at – I can try to address, it's something that I have looked – thought about at least so, these sorts of contracts are called contracts of addition or standard form contracts. Now in English common law which is also what we follow in India, such standard contracts are usually read against the

person drafting the contracts. So, there is scope there to challenge such contracts. There is also the concept of contracts being void for uncertainty so you know, these are – there are grounds definitely. It hasn't been done so far, it hasn't – I mean these particular contracts obviously have not been challenged in India successfully but it is – these are definitely grounds on which you can criticize them and perhaps even challenge them in court so, yeah these are definitely valid points.

Q: Public interest is actually increasing the urgency of these issues so, how do you actually regulate the public interest and define public interest because I think it is unclear to the masses what is public interest and how does it differentiate from a private interest so, a PPP arrangement for example is assumed to be good in the eyes of the public, whereas it's actually giving away public interest and public benefits to a private party in perfect surety to literally look and create an East India Company so, how do you actually you know, address the issue of protecting the public interest for the larger question?

C: Yeah you know but I – I think you know, there are some traps we have also fallen into. For instance, the idea that government is inefficient and therefore it has to outsource functions – it's not only in data related tings but many public services have been handed over like this. So, you say we can't do it and therefore, you know, a Company's Act where we changed the law and we said that 2% of the profit of certain companies have – have to be put towards CSR and the kind of things which come under the CSR are what the government is supposed to provide to our people and you privatized us. Saying that government is inefficient, it's incapable of doing many of these things and therefore it should pass that on to somebody else so that it can be delivered properly and done properly.

One thing that I find is that if you give this kind of power and responsibility to somebody and there is no liability for nonperformance it becomes an easy way of experimenting on populations and in fact I am not even – no longer willing to even call it experimenting because they are not looking at the results, they are not – they are just looking at roots for profits. So, they are not figuring out, you know, in the UID thing for instance we asked them, "how many people who – how many enrollments did not fructify, this is they did not become numbers?", and they said, initially they said they don't know and then they said, "yeah it's a – actually it's about yeah when 80 crores had been generated, 8 crores had been rejected, when 90 crores had been

generated, 9 crores had been rejected", so we asked him, so what have you found off from it because you are experimenting you are saying this is an experiment so, have you found out why that happened? Are these people really people who ought not have been enrolled or is there something the problem with the process or are these people duplicates who keep coming and trying to get back on to your system or do they not exist at all and some enroller is doing some you know, hanky-panky somewhere? And they said, "actually they don't have a feedback loop", which means it's not an experiment, it's just finding different lanes and routes for profit, if something doesn't work you drop it if it works in a certain set of people, use those set of people. So, the levels of unanswerability has just grown phenomenally so, it's – I don't think, you know, for a country like ours which makes laws by the dozen, we have nothing on any of this and nowhere it's liability coming in. So, when we are talking all these things none of these matter at all because in any event if everything crashes you know, you disrupt whole systems and rest of it crashes, they'll say, "tough luck", shrug their shoulders and walk of it whatever they have and that's it. So, it's more than just a public interest, that's what – that's all I'm saying. I'm saying that it's not just the idea of the public becoming private, it is about total abandonment of principle and norm where you don't have any answerability at the end of any of these systems.

Q: So, have they rejoined there to guess, it's basically a conflict of interest that has emerged in a huge way in the transfer of public to the private. So, if you see even in the case of GSTN –

D: You can see that it's a private company, non government private company which is going to collect the taxes and you know, manage –

C: And make profit also.

D: And who are the people on the board of GSTN? They are people who are current or Ex bureaucrats who have actually handed over the contracts to the GSTN and in the case of UIDIA and MPCI it is again the same scenario. So, these are people who have demonstrated high conflict of interest and shamelessly. So, I think you know, if you have a scenario like this then how can say that even with the law that privacy will be protected or for that matter the interest of the nation will be protected, forget the individual interest even the interest of the nation will be not be protected because it's not being protected in this case.

A: I wanted to make a couple of points with regard to the framework that D was talking about on how big data is creating or distorting, how we look at privacy and some of the solutions that we could have, so in my view one of the problems with the consent notice and consent frameworks is the larger problem is one off scale because we cannot – the kind of privacy notices, the language in which they have presented to us the length of those notices often they might not be in the language that the data subject understands at all so, those are again problems with free data, big data in somewhere and big data I think exacerbates it with scale because if you have to give consent at so that of every waking moment of your day and a lot of times if the consent is completely implicit and you are not even aware that you are giving it so, that's the sum of a additional layer of problems that it poses. My question is when we look at something like Habeas data as a solution I mean it largely comes from the idea of empowering the citizens further in some sense right? But often the – and you spoke about the RTI but even within the RTI if a question – RTI is more than right to information what it has turned out to be is a right to access documents so, the State is not going be in the business of actually creating documents to answer the question's post and very often when we are talking of the question of how data is being used for the purposes that it's being used for then if there is a high possibility then there will not be a clear document trail which the State will have at its disposal to respond with. So, that I think it has – it becomes a large problem and especially with big data because the manner in which the processing is being done is often unclear to even people who are doing it. So, in that sense I think along with a rights framework where we strengthen the existing rights there might be a need to think about in some sense a more paternalistic solution where there are obligations are imposed on data processors on certain things that they have to do rather than looking at empowering the individuals, I think regardless of how empowered we are we won't have the capacity to question some of these things. I think we have to have positive obligations in some sense.

D: I completely agree with you there. So, I don't think big data is going to solve – oh sorry Habeas data is going to solve all the problems of big data, in fact you know, problems such as consent etcetera will not be solved with Habeas data at all. It's just one of the tools we could use to reduce our anxiety with big data and privacy issues it brings up and as far as the RTI Act is concerned the problem there is that and that's something I didn't speak in my first this thing is also something C mentioned later

which is the exceptions in the RTI Act are humongous you know, if you have like a very large list of exceptions and that may sort of frustrate your efforts because if say you want to know what sort of surveillance data the government has on you, you can't get that under the RTI. They'll just say security and that's it end of story. So, it's as I said Habeas data, point was just to start off a conversation and see if we can maybe modify this tool to address some of the issues.

Q: See, just one comment, as you can guess – for some of us it's a continuation of earlier discussions, okay? We keep talking about these things in our work time and leisure time and so for those who were not part of that conversation, if you have specific questions about different arguments being provided here and kind of because it's – a lot of knowledge here are assumptions that the other question is a way of certain things, certain organizations, certain people and so on. Anytime anyone has a question regarding the details of things please feel free to ask okay? We do not want to increase in between like we are having a kind of a spoofed conversation in front of you, yeah? So, please help us not to do that right?

Q: First I just want to thank you both for some excellent presentations really, really fascinating knowledgeable and I just – it was just another follow up on suitability of Habeas data and ideas in this world of big data particularly because what also matters when we think about big data and the use of action intelligence machines learned to interface about this, it's not just my data that they are using to learn information about me, they're using kind of my neighbors and other people around this influence game you know, from data around me. So, getting a list of what they know about me, doesn't tell us what tomorrow they will learn about me based on what my neighbors are and this is kind of becoming it's quite a challenge I think more generally in data protection in law of part and powerful ways which I'm struggling with I don't quite see the answer to. I don't if we see any other ways forward.

D: You know, quite frankly there is no answer to that what you've said is a very – what you about - the point you have made is a very valid point that you can't get the future information. The only thing I can add is that if they have used your data along with your neighbor's data before till the time you've asked for this information, you'll get that information because when you get the information of what data they have you also get information of the purposes for which they've used it. So, you may not necessary know that they've used it along with your neighbor's information but you

may get to find out what use they've put this information to in the past but yes of what future uses they intend to put that information is not something that you'll be able to figure out at all. So, as this is why I keep emphasizing that business data is only a very limited solution, it's a very limited took but just because it doesn't provide the perfect answer doesn't mean we should discard it and I think big data is such a complex issue that it's highly unlikely that we'll get one you know, answer to the entire problem so it may have to be number of things cobbled together.

C: This idea of big data and I think we shouldn't just accept the terminology as it comes to us. It's worth it okay – I think we should be little careful because see the – what big data seems to ask us, we have to imagine is data that is not – what's the word that's not specific I mean it's – granulated yeah it's the granular data so that is not granular data and therefore it's not actually – it's not coming to you, it's not coming to you, it's not about you, we don't know, it's all anonymised, it's all you know, it's just meta data and that's a myth as far as I can see, it's not true, that's just one statement I want to make a leave with that.

Second thing is that when I heard when I attended a meeting on big data when there were all these corporal sitting there and saying we are the good guys and you know, big data will help in multiple ways, they were referring to the Microsoft I think, experience with Pancreatic cancer and saying that you know, when some – when they went to see you know, how many people from which area were asking about pancreatic cancer and it what when they went back to see what was being asked years ago, two years ago and they found that there were certain kind of it so they were able to see that symptomatically when you know, two years ago people would have been asking for certain kinds of symptoms and asking what does this symptom ? And then it turns out that a couple of years later they actually contract pancreatic cancer. So, they were saying that you know, with big data we'll be able to have preventive method. So, then I'm thinking really Microsoft is going to be my preventive doctor so but this is the part of that marketing of the idea of big data and that they should therefore be allowed to gather data, to retain data and to create various kinds of algorithm which will allow them to do multiple kinds of things because these are our benefactors and our protectors and you know, whatever. So, I think, you know this, which is why I think this idea of big data I'm not willing to accept the term as it is because it is coming with a certain innocence saying that you know, I'm innocent of who you are and what

you're doing and whatever but I can just you know, provide pictures of what is happening in the world and then you can then recast your world to whatever so, I'm just saying let's not take it for granted that it's as you know that – and if you don't have a definition for it then we know that there is much we don't know and what is being proposed with it.

Q: My questions are little bit of a history question. I'm just thinking every time we are talking about the idea of social security and how this is all linked to or at least that's how it's told, this is going to be this great social security more than you'll be able to access, all kinds of things. I'm just thinking about in a peak self digital data world we've still talked about social security in terms of PDS in terms of all kinds of things and this narrative and the way that it gets conflated with corporate profit making enterprises, I'm just wondering how does this come to be conflated with each other? The idea that there could be a private of way or in the sense a non-governmental way of establishing social security.

C: See, at one level it is about marketing. It's about saying that we are going to intervene in systems which are not very good and we'll produce much better results than the system will and you're saying that doing – it's shooting from the shoulders of the poor. So, if you say that you are doing it for the poor, it is very difficult to say you should not do it. That's how we began thinking that you know, they're doing this. Then, we find that actually it's not even that simple there are two things that have happened through this kind of process. One, the State becomes a customer. So the State has to – you know the State then or the State becomes the medium through which customers of technology are created. So, every PDS shop has to have a POS you know, point of service machine, you know, you have banking saying and saying you have to have various kinds of machines, you'll have to have, even the digital and I'm going to pause here I'm sure I'm going to forget my second point but I'm going to go back anyway, I read a book by this you know, you guys will know, this Heather Brookes, she in her book on you know, where she has a line there and I've been trying to follow up on that line if it can help it will help, she says that in 2002 I think in Lisbon, they had a meeting you know, like they had all the countries meeting and the technology companies went to them and told them that, "listen after the dot com bust it all you know, where are we? We can't do anything with the work that you have, you don't have customers with" – and that's the time that the governments agreed that

you know, there would be a mutuality of interest and that you help us we help you, so governments agreed that they would bring in, make, give these technology companies work within government systems and soon after that you find that from 2003 onwards all developing countries have suddenly this e-governance projects and everything getting on to e-governance, this is not something that just happened. It happened because companies needed and which is why this slogan is so easy to understand that companies were collaborating with the State, State collaborates with the companies and they live happy ever after and the rest of us are forgotten.

So, that is one about the – now I do actually remember the second which is that when you think of something like Fintech companies, which is what Nilekani is investing in for instance, they need – what are they saying all the time? They need all the monies that are being given you know, they don't want any subsidies, they don't want any money going out to the poor, they don't want services going out to the poor, they're saying anything you have you put it in to their bank accounts let them come and spend with us. Let us be the ones you know, why is government intervening in all this systems? Well if you look at the PDS systems the private companies are completely out of it and they are saying you can't have a circular thing like that when we are out of it so you give the money to these chaps. So, the disruptions that's happening in the PDS system for instance is to destroy the PDS system so that the money will go and you look at what they are saying, they say we will give credit, there will be a consent, the money will be put you know, the government puts in money into and now with NPCI which we will talk about, money moves from AADHAAR number to AADHAAR number not bank account number to bank account number, money is therefore put into the bank account number – bank account which has attached to the AADHAAR number and so the moment the money drops it is shifted you know, so you give credit and then you keep you know taking it back. So, what are they saying microfinance 22% to 24% they had to pay because even though they got a collective to repay and there is this moral force and what not it works within the collective they still had to go there and try and get it, there's still some transaction cost. So, they say no, no transaction cost so we'll give it to you at low rates because the moment the government – it's now only for the government to only put in money into the bank account and it will get automatically transferred to these chaps who'd given credit. Who are they giving credit to? Small you know enterprises, the poor and we are the great guys who are going to do work for the poor and grab their money which comes

from private – from the government, it will go directly into private hands. So, there are reasons why their social security system has been addressed. It was actually not being addressed; it was being attacked to be destroyed and to be converted into something else which is an opportunity – business opportunity for others. It's the most cold blooded thing that I have seen because you use biometrics knowing that it will not work on the poor and you destroy the system through that process and you get yourself e-sign an EKYC and digital locker and grab their money, that's why social security has been important for them.

Q: I just got a quick question, D, so, you talked about how Habeas data is mostly applicable in – when it's public if it is a government and public what happens when some private entity like for instance WhatsApp transferring all its data to Facebook because have you thought about this because in some jurisdictions government has stopped them from doing so but in the Delhi high court we didn't really succeed on that front so, have you thought about that?

D: Yeah I have thought about that in fact I've written an article on Habeas data, it should be up on the CIS website in the next week or so and I have addressed that issue in the end there in that article, the problem with including private entities in Habeas data is that when you are approaching single point of contact to get all your data now the government – you can approach the government and you can technically say that, "the government should know exactly where my data as in how many databases it has my data on?" The government should be able to check that and that is an assumption under the RTI Act as well because if you approach a particular ministry, even if they have five different departments where they have data, they'll send it internally and get you the information but in Habeas data when we talk about private entities it's going to become very tough actualize that right because the government will not know. If say you have a – say SARAI has a database and the government is aware of that, SARAI for some reasons shares it with CIS and does not inform the government, you know, through – there is a practical problem there when you're looking at applying Habeas data to private entities. I'm not saying it can't be done because apparently there are countries which do that. The other problem with habeas data is that most of the literature is available you know, Portuguese and Spanish articles so, there's very little English literature on it so, I was trying to find you know, exceptions, the accepted

excepted to Habeas data and stuff and it was not very easy to find it but that is something we need to explore further on.

Q: But I think the question that you asked might also be related to the whole point about citizen versus consumers that C made. So, the way we understand the rights framework at least the jurisdictions like in India and even in United States is those rights are only available to us against the State, they are not available to us against private parties whereas, especially in the context with privatization of a lot of public services we're seeing and especially where we have private parties being in a much stronger position of power, there – there is reason to relook at that and again I think that's a complicated legal question, you know, how we approach – what kind of legal solution we suggest for that so, it might be very difficult to bring in private parties within the rights framework because we have evolved Jury's prudence which has time and again limited that but maybe we can look it – so and when we think about initiatives like privacy bill or having a data protection framework which includes not just the state but private parties as well, they are more in the nature of consumer protection solutions where we're viewing a data subject not so much as a citizen but we are actually viewing in as a consumer and we are holding parties dealing with the data as accountable under another system of law.

Q: Sir, just to quickly respond to that I think there is something to be sad about thinking about an entity Facebook for instance, it is in a way to hang on characteristics of a very public space right so what we say State and public the fact is that, that is space can all differ a large majority of people are on – a lot of people are on. So, even to say and something like to state one could possibly in the future make an argument but those kind of entities, certain kind of entities may come in, not every private entity but maybe there is a key.

D: Yeah, I mean that's absolutely right because when we talk about something called public purpose you know that's – it's not very specific concept so it is very possible through Jury's prudential here evolution to bring a lot of some private entities who perform public purposes under the this obligatory framework whether it is Habeas data or RTI or whatever but it hasn't happened so far and it is something that I think it will probably start happening as and when the people realize the problems that will come up with -

C: Just want to think it only - I think we should go back and take a look at the Bhopal decision of December 1986, that was the one time that in a different context but it was a what economic centers of power and whether companies of that nature can be brought within article 21 of the constitution and while that little – it hasn't developed, it's a very important decision so we shouldn't lose what we have if we can.

Q: Going back to what C was saying a little earlier about government supporting the software companies and all that, actually in the case of Bangalore we have a earlier start – start to that when there is something called e-Government's Foundation which was formed by Nandan Nilekani and Srikanth Nadhamuni was running it but if we go a little further back actually I mean though we are talking about governance and government can we look at statement which came out I think during the United Front government time but I'm not exactly sure but this was a conference of Chief Secretaries and Chief Ministers on efficient , responsible and administration and government so when you have a discussion at a very high level where you are actually talking about government and then this transition to governance which happened actually subsequently so you actually need to – we need to look at why did this change take place. So, you already had the Asian development bank and probably the World Bank already involved in many of reform projects especially in Karnataka and e-governments foundation got involved immediately with municipal reforms, they introduced a series of software for websites for revenue, for property tax, for all kinds of issues and scaled it up under the JNNURM which is the – when it was called the Municipal mission mode project something that E-Government's Municipal Mission Mode Project so, I think these links are very – very much there but the change in direction from government towards governance and then towards e-governance I think that is what something we need to really look at.

Q: So, I primarily had a question to sort of better understand like both your positions I mean if you were to say that like the entire thing that is happening on AADHAAR if both from the government side and from the corporation side is driven by incentives right? So, corporations are clearly doing this because they have an incentive of profit, the government is doing this because they think that this will make the system more efficient or will allow them to do better or not, so what I'm trying to sort of understand is:

Is the nature of the incentive for why these entities are doing is that very major problematic and should that nature change or alternatively can the manifestation of these incentives which is it's okay if the incentive is profit but there is some form of regulation as to how you can achieve that profit and what you can do with the information that you can collect etcetera, etcetera should the measure – like it should be carried out and I mean if the second one I think you could answer but for the first one, if you necessary the government needs to have a different incentive for carrying out such measures taking it to the good of the people, the betterment of the society etcetera, etcetera then do you think that if some of the actions that are currently being carried out by the different private entities carrying out things under the AADHAAR were to be carried out by the government entities that you know, for example fell on to the RTI was aware subject to more public over sight etcetera, etcetera. The – like to what extent the problem that currently exists with AADHAAR not exists in that sort.

C: See I think one reason that we reject this whole this is because we have been fed with lies, lies and more lies. You cannot have public policy being made only on lies. So, there are many things beings said and many things which are unsaid. The things which are being said are not true. It is not being done to improve and it's you know, they said that probably voluntary, all of us know how voluntary it's been. They've said it will be inclusive and anyone that has gone around to see who is getting excluded and who is getting included can see whether it's inclusive or not. They said it will be – so that you can have more control over your life and you've now found actually the – new norm is of involuntariness, you don't have a choice and you have – you are just on systems and so – and it is completely unregulated and deliberately so. It is not and when you look at bill that ultimately came because of all the battles that we have put up, you find that, that bill takes away even more economy then without the bill. So, there are – the – that's one reason for saying that we reject the whole system, there is another reason for saying we reject the whole system. There is another reason for saying we are rejecting the whole system which is that you know, already we are in an age where it's very difficult to maintain your security and your personal space and the sense of your you know, some amount of freedom, it's not easy when as it is.

On top of that you say that you are going to create a database, keep it digitally and expect that I'm going to feel secured under that. A data-basing of a whole population on untested technology and on a technology where we've been told time and again

that, that which is electronic you know, and then you can't say electronic and secure in the same breadth, you can keep trying encryption then a little somebody will hack someone will take something away. Thirdly these are being done with companies which are highly suspected because there we don't to have indigenous technologies on this and we have players who are coming in from who we know who have close links with CIA, FBI, French Government and we don't seem to have any – and when they – if I tell you that an answer to an RTI request about how it is that our data about out citizen is being handed over to foreign companies the response was that we have no means of knowing they were private I mean they were I'm sorry I keep saying this – that we have no means of knowing that they were foreign because they have a local address and that's all we ask for and all you need to do is to Google and you find that they are in the corruption index so if that you know National Corruption Index and I am like, "Really you didn't know", I meant that's you know, that's use of yeah and -

Q: They don't use Google.

C: Yeah they don't use Google that's true and the explanation that is given, every time we say that there is this database is dangerous to have these kinds of databases of people is you know why do you keep complaining about us what about Google? What about Facebook? Like that justifies everything. In fact Google is a huge problem for many of us and its closeness with the U.S. defense establishment is something that we choose to forget because we have forgotten how to live without Google, we don't want to know but the fact is that there are problems there. So, you know when a State starts collaborating in with – you know Mr. Nilekani was a you know was a industry man who went in not – you know in the rank of a cabinet minister but without being a cabinet minister, what's the difference? If you are a cabinet minister you are answerable in Parliament. If you have the rank you have all the privileges, you can attend any meetings that you want but you don't have to answer the public at any point. You don't have to answer in Parliament at any point and that's the kind of system in structure so, it is processed, it is product, it is lies, it's a range of reasons why this is not okay and we are seeing today that a set of people might be able to get on to it and use convenience but many of us you know the middle classes have no value for freedom, they will say what will I do with my freedom and they believe therefore that the poor have no value for freedom they only want food and whatever and they certainly don't want privacy because we don't understand what privacy is? So, this

you know, distorting and what we are seeing is a completely distorted image of our life and that's what's been fed to us to convince us that this is a good thing, we are contesting all those image making act you know, efforts.

Q: My question is related to the law so we can take it on later. One okay I can just phrase it you know, it is skeptical question because if you look at it from a common man's perspective. If you look at the prevention of corruption act actually it's protection of the corrupt. If you look at the representation of people's act people don't matter, political parties do, if you look at you know, the environmental protection act the – it's licensed to destroy the environment. So, if you look at practically every act that you know, the common man will view it's actually doing counter to what is intended or what would be a public interest so, how does one protect if there were to be a privacy law how do you ensure that it's going to actually address privacy and protect it and not actually be a way to destroy the privacy so, should it actually be a you know, licensed or data act or you know something else I don't know.

A: We break for tea and coffee quickly come back here in few minutes. One five.

Session 3: Digital ID, Data Protection, and Exclusion

E: Good. Thank you. My name is E I have been a member of the European parliament and in fact, I was a member of the European parliament at the time when the parliament was constructing its new data protection laws for Europe which is now the general data protection regulation. And it's accompanied by a directive on the use of personal data in law enforcement activities which I expect because it's a quite large concession by the member states of powers to the EU to interfere with law enforcement relationships with citizens. So, that will be extremely interesting to see what the effect of this directive is on member state policy. But I've been asked to talk even about the background for data protection regulations in Europe and why we have these laws especially in the context of the ongoing Indian discussions on the AADHAAR and UID and whether a privacy law should be enacted. I think it will be helpful to have some of the backgrounds from the European situation and how we actually got to the point that that data protection legislation is now pervasive.

So, the first data protection laws emerged in the German [Inaudible 1:18] Hessen in 1970 and in Sweden in 1973. And in fact they were enacted specifically because the introduction of electronic systems in government allowed the government to [Inaudible 1:30] to a mass, large quantities operational data about citizens where they live, their social number, what their health status is. And the government perceived at

the time that it needed to regulate its own relationship with citizens to ensure that such power was not abused. The discussion on how collection of large data sets impacts the relationship between citizens and government is also visible in the council of Europe convention of data protection from 1982. The impetus of which is, collections of large sets of data have the capacity to give somebody, namely the government, a large amount of power over individuals and we need somehow to have a constitutional protection from the exercise of that kind of power.

So, in practice we can wonder what's become of the data protection laws and the different member states. And they've developed in fact a very different theme. So, while in German the concept of doctrine showed data protection is extremely strong especially following a constitutional court case in 1983, where the protection of personal data or informational self determination was elevated to a fundamental right of the German citizen. In Sweden it's in fact turned out more as the legislative framework that we expected to be followed but we don't really have the mechanisms for doing so. The general data protection regulation goes more in the direction of the German concept of what the data protection right should be. I should add, data protection was also added as a separate constitutional right in the EU chart of fundamental rights that entered in to effect in 2009. And it still remains to be seen whether the European court of justice makes a distinction between the right to privacy which is a separate right and the right for data protection because actually at this time they've mostly been dealt with simultaneously.

So, I know that there are some pushes from, for instance European data protection supervisor to see data protection as the toolset by which individuals can choose how to exercise their right to privacy. But it's also very clear that there are some cases where the right to privacy comes into play and where data protection really doesn't matter. One of those things would be for instance how can a government dictate that its citizens are presented on a passport. It's not so much a question there whether the data is safe but about what the data is.

Now, I noticed in the preceding session that there were some discussions C began by addressing this difference between data which is true and data which is false. I recognize this discussion a lot from Sweden in the last two years where we've been discussion defamation law and the ability of defamation laws to protect adequately individual privacy in online environments. So, this is essentially the concept that if an

individual spreads false information about another individual then the defamed individual should have a tool for somehow prosecuting or correcting that error. But the law gives very little protection for those people who find that true information is given about them in online environment so being used to defame them. In Sweden this has primarily been an issue in relation to revenge porn or information about sexual behavior of people which may be true but it might also be something that you don't want everyone to know. Just because it happened it doesn't mean you want everyone to know about it. And it's been through the point in Sweden where we've had to introduce separate criminal provisions to ensure that people that have been exposed to an injustice have a legal means of recourse.

I shall also say that in the discussions on general data protection and in relation to big data, there has been extensive academic debate in Europe on whether the general data protection framework is enough and sufficient to deal with the problems of big data or particular automatic discrimination that arises in algorithmic environment. I think the general academic consensus from legal scholars will be that it is not. I have increasingly come to believe that in order to get a full protection for individuals in digital environments probably what we need is a mix of the American approach with discrimination laws and the European approach with data protection laws.

The data protection law ensures transparency and accountability in data processing. It means that individuals can foresee with whom they have relations and what those relations are meant to be. A discriminatory framework gives the individual action when the relationship does not turn out the way that the individual foresaw. In the US you see this most prevalently in the financial regulations. They have, you cannot discriminate when giving credit on some grounds like ethnicity or race or religion. You see it also in healthcare in the US, they have these laws. As far as I've been able to determine it's a bit more messy because they're basically going sector by sector and seeing what kind of discriminations wouldn't be desirable in each particular segment of the economy. So, I'm assuming the American legislative model would be much more time consuming and then in particular it doesn't give the information security protection that the data protection law of Europe does.

So, probably a mixture of the two systems would be the way that I would hope for the European Union to advance in the future because even though I am confident that the general data protection regulation will stir up a lot of problems and give individuals

additional rights. I do not think that they will be sufficient rights to deal with the entirety of the problems that individuals might face in an increasingly digitalized world. But in order not to hog up too much time, I will end there and leave to F to present some of his technical observations.

F: Hi. I just want to give a brief introduction of what I'll be covering. I am myself in IT and a privacy novice. I use all sorts of software and tools which collect data including Chrome, Uber everything, so, bear with me with all that. I also intend to cover briefly on data protection and security and privacy in our context like what that have been and how it should be. And effect of big data on welfare state, so, what are the things that could change because data gets collected and how it affects us. And the exclusion, so, here what are the things that get excluded based on your identification and what can we do about it. So, digital ID today, even though we've been with digital IDs like everyone of us would have had PAN numbers, those are merely for recording purpose which can be queried for account and compliance and things like that whereas the newer digital ID the UIDI AADHAAR is actually a transactional one. So, instead of your PAN number which also was populated in multiple databases was a passive one with which you cannot actually do a transaction whereas with your AADHAAR, this gets into a transactional mode. So, for which you would be held accountable if there are multiple records and multiple databases. You would actually be proven that you actually did these things even though those could just be an effort of cyber security breach.

So, what this gives us? It gives us seamless user experience. So, it will start from say in an airport you could just go ahead and place your fingerprint and pass through security. The seamless use experience also gives around a cost. It comes with a cost both in terms of money and in terms of privacy. It leaves digital footprint across databases and we also tend to increasingly be reliant on information system. So, the basic human factors like trust would cease to, would tend to go down and we would increasingly rely on systems like on basic values of trust.

So, next, this is data protection. So, what do we need to do for data protection? So, one, first thing is data awareness. So, we need to have citizens be aware of what all the data that they are actually giving in every time that they give in. then the next point I want to briefly touch is data sensitivity. So, the people at the receiving end who are collecting the data should be sensitive enough about the details of data and what they

could cost. The third thing is of course cyber security, so, when we are storing data across databases we expect data to be secure. And the other thing would be the laws around it. So, both data protection laws, privacy laws and cyber security laws. So, a brief example that I would refer here is the recent debit card hack that happened. So, we all know that 32lac cards got hacks but what probably many of us wouldn't know is, even that there was a list of 84000 Canara Bank account numbers with debit card numbers, anonymized debit card numbers that got circulated on WhatsApp saying that these are the account numbers whose cards got compromised. So, here it's a problem with both data sensitivity and data awareness – sorry, data sensitivity more than cyber security.

So, it's one thing that 32 lakh debit cards get hacked. It's totally a different thing that a person who is sitting in Canara Bank gets a list of all the debit cards that got hacked, publishes a PDF and sends across in WhatsApp. So, this is total insensitivity in data probably done with good intentions to share information that your debit card got hacked but in the process it sent across the entire list over WhatsApp. So, it's important we understand data protection as more and more functions of our life get digitized.

Next is, in the name of welfare there are good and bad things that can happen using national identifiers. One thing that we've seen in the computing world is more and more data gets collected and that is being propagated and that the argument for pro data collection is that you get a greater personalization. So, Google collects all the data because Google can serve you relevant ads. So, extension of that is when you collect citizen data, the next level of post data collection would be personalization. So, personalization could actually mean pricing and taxation. So, something like, tomorrow you would be, instead of having a POS machine you would have a POS machine with a biometric fingerprint. You would place and it will determine the price and determine the tax. And it will initially sold as welfare because people will probably think that, people who own this X or Y car should not get water for this much rupees. That will tend to – a greater level of personalization which will eventually lead to opaque tax rates and opaque pricing.

Then we could also have large amount of data that is getting collected on education and on health. So, on health the scarier stuff is this is ESIC, they collect AADHAAR data and they also have an entire system that puts online about the prescription, insurance

and all this data is out in public. So, in US there is HIPAA which strongly advocates privacy of healthcare information whereas here we have the state actor putting out every piece of information on people's health out there. So, on education it could mean that we know that the school student's are being asked to give AADHAAR and take exams. So, a more rigorous form of data collection could be even be like, what are the individual split wise marks that the person got, what subjects the person is strong on. So, this kind of information can be collected out of the mark sheets. And this is actually a very standard periodical tool that teachers use to advise students but imagine this data getting into a database and that database is tied to another. So, tomorrow any employer or not just employer, anybody can actually know what you actually know or what you don't know.

So, then there are good things with these either like, on education the data collection is not bad if the intention is just to make the student learn or even on the fence there could be two sides of the coin where like the, healthcare data is being taken by pharma company to produce drugs. The optimistic side would say like, we will end up with lesser and lesser diseases, the pessimistic side will say we'll have greater diseases because companies want to use the data and make money out of it or anything. The other thing could be like rationing so, we know that AADHAAR is linked with PDS and it is supposed to eliminate corruption at the lowest level and ensure foot security. But we don't know how efficient it is or I don't know how efficient that is but what we could also have with the national ID system is, we could also ration other things and it will probably start with liquor and cigarettes because these are the things that get taxed way higher because they are considered to be evil. Once the system is in and then it's a matter of time where the state decides what are things that need to be rationed. So, the commodities could be replaced and anything and everything can be rationed individually. So, your availability and access to goods and services will be very personal.

In the name of welfare this is a Twitter tag that pops up every now and then, 'follow the money'. So, we here could, we were briefly discussing about who made investments into what and how that impacts us. So, the same thing can also be done by governments. They can track us, what we are spending and how are data flows and you can freely interchange the words data and money. So, if they follow the data or they follow the money, they know us. If we follow their data if we follow their money

we know then. So, that's going to be the norm. And universal criminality is something like, so, we had a brief version of this in 66A where like the law was absolutely vague and everything came under the law and people were arrested for liking things. We actually have probably many such draconian laws and we get escape out of it merely because of lack of data and evidences. With national ID systems and cross functioning databases everybody could be made a criminal or you could be per sued any legal action against because you are leaving some prints of data which is probably illegal by an over arching law.

So, it may not affect 2016 it could affect the 2020 elections. For us, the same thing could be said like, it may not impact 2019 but it could impact 2024. The optimistic side of it we'd say like, we eliminate corruption, we eliminate black money. We bring in electoral reforms, we have a truly great, democratic function. You could imagine the pessimistic side, what can happen with this kind of data collection and 2024.

The other notion is the data collection systems or the data itself is not for profit at core but they are surrounded with profit maximizing shells. So, to give an example with the data, the AADHAAR system says that, we collect the data but we don't give the data to anyone. We only do yes or no answers, we provide yes or no answers. And that is not for profit, we just provide for convenience and authentication whereas with that yes or no answers people could build around profit rich datasets. So, we actually have a non for profit core and we have multiple layers of profit maximizing shells. And this could also be said the same way with UPI where NPCI could be a nonprofit whereas the multiple layers that come around NPCI could be profit maximizers both in terms of data and in terms of money. Exclusion, like we all know there are bunch of things where AADHAAR is being mandated and we are put into trouble and we seek solutions of escaping enrolling into the AADHAAR. So, that is one form of exclusion where we are currently excluded or product and services, government services today maybe. With Jio SIM card it's probably even a private service that got excluded. Like, you had to have AADHAAR in order to get a private SIM card.

The other forms of exclusion include language and digital exclusion. So, language is, even though there has been a digital India program and multiple products like these like AADHAAR and UPI, mostly they have been only in English. Sometimes they get along to Hindi as well but they still do not consider the vast majority of people who don't know either of these languages. So, they exclude people who don't know both

these languages and that exclusion also costs, it doesn't help their own goal of providing convenience. Digital exclusion is where we build more and more complex systems and we simplify the system so much and we create more and more opaque systems or rather the shells around the core and make it very hard for anyone to understand what these systems are and how these systems work, what are the impact of these systems from a privacy perspective, from a technology perspective, from a business perspective. It's very difficult to actually understand the system. Most of these things are being passed as tech and saying that this is how tech operates but that is in a form of excluding probably everyone else except developers from participating in design of these solutions.

The last one is stakeholder exclusion. I happen to take India's tax survey where the survey actually had mentioned stakeholders as investors, entrepreneurs and regulators. I think extending the argument C made, she said like, citizens are getting converted into consumers. I'd further extend that and say, people are mere objects in this software world and it's a pun if you are into the programming language concepts. So, we the citizens are not a part of these designs of these software so what is being fed is, we have a software here and you can develop apps on top of it and we will hold the platform. And these platforms are not opened participatory and democratic.

So, for language exclusion I just made a brief post which said – but there are positive upsides. The language exclusion is partially solved like, with the advent of UPI it's probably we had the first Tamil mobile banking app or any banking app in Tamil. Even it's hard to find chalans these days in Tamil whereas with technology this has been possible. So, technology per se it cannot be evil. The design of the technology can have evilness in them but we need to find a way out. We can't say that we'll not use technology and that's not going to solve our problems. We need to use technology but we need to see how that technology can be more democratic participatory in nature. So, what can we do? So, educate people about these basically privacy, data protection, how these stacks that come around us. Participate, try and see if we can participate in policy decisions. Demand access, so, demand access is, while there can be a digital access built around these systems, there should also be a free and open access that is available for people who want to build their own say, privacy compliant solutions.

So, like I am not asking Internet Explorer or Chrome to be shut down, I'm just asking your operating system should also support Firefox. So, it's basic like that. So, you need to get access to these technologies, a free and open access on top of which I'm pretty much sure that the open source community or the free software community will build around apps which are privacy complaint. Not just open source community, any community which wants to build apps for their own interests can do so.

The last point I want to mention is instead of merely criticizing these stacks, we should probably go ahead and build shadow stacks which are something more like shadow parliamentary report or a shadow ministry. That's it.

E: So, is it possible for me first to come back to the question that I know was raised in the previous panel about what's the actual efficiency of the European data protection framework for citizens in European countries. So, the first observation is there is 28 European Union member states and the implement of data protection law is very different because the culture is very different. The administrative culture is different, the way in which the government organizes itself is different. We've seen in the last few years, a few member states particularly in the Francophone parts of the European Union, acting out against social networks collecting a lot of user data. The Swedish data protection authority is certainly not doing any of the sort and neither is any of the data protection authorities in eastern Europe nor in the UK. So, one could then say that the data protection authorities, DPAs, in the Francophone countries are acting to protect user interests but it's also true that they're not investigating government authorities as much.

So, France is now for instance in a state of exception for more than a year which means most human rights don't apply there. The only right you still have is basically, they can't kill you arbitrarily. So, the DPAs there have been overly focused I think, on some American companies that they've designated as bad. For [Inaudible 9:29] reasons they don't employ people in Europe for instance this is a big deal for a lot of European legislators. They don't pay taxes in Europe, this clearly also is a source of contention. But are they really the biggest threat to privacy or data protection in the environment we live on? I have difficult seeing that that is the case. The Swedish DPA is hindered by a legislative maneuver implemented in 2006 which causes them to be unable to act unless there is a specific case of abuse that was detrimental to the citizen. And because the data protection authority often can demonstrate that the

protection in Sweden is effectively really low. The DPA is understaffed, it's under resourced, it has no technical competence at all. Their entire cloud knowledge was derived from Microsoft as have been reported. And also when it comes to government proceedings they have very few tools that they can do. For instance they have this specific instruction not to impose any kind of sanctions until they've engaged in a very fruitful discussion about voluntary measures that could be applied to remedy the measure.

So, we'll see what happens with the general data protection regulation. It's at the aim of giving the DPAs more teeth but it won't enter into effect until 2018. And one of the things that was introduced in the data protection regulation which almost regardless of whether you advance with a privacy law in India you should definitely try to make part of the consumer rights framework with respect to information security is incident reporting. So, that people find out when something does not proceed as planned. And even if this is not sufficient to get an understanding for when things do proceed as planned which I think a lot of the big data discussions are about. Still finding out when something goes wrong is the, informing consumers about that or individual citizens is the first step for individual citizens to gain awareness of the kind of new environment that they are in. And so that's part of the GDPR, we won't know probably for a number of years after it enters into effect whether it will have the intended consequences in the European area. Normally I guess one could say the answer to your question is, it depends or not really.

Q: So, I have two questions, one is for E and the second for F. So, the first question is that, there is a lot of public function that needs to be audited and it goes beyond simply asking a document. So, you need to actually audit for example, how government spending happens and we discussed a little bit of that earlier in the morning. So, in that context, how does the EU deal with access to information which will allow us to audit government function? Secondly in a private context, we often enter into an agreement for example contractual agreement with a bank and we want access to data, our own data which we may not get. So, what is, how is that made accessible or how is data about whether the way in which a function is undertaken by a bank audited and the audit report be made public? Whether that should be made public? And then the second part of this is basically, if you were to need information

for any arbitration purposes to get a fair trial, how do you actually access such information? So, that's a question to you. shall I put F's question straight away?

So, F, I actually want a clarification. I'm not clear about what you meant by the difference between PAN card and AADHAAR in terms of transaction data because I would have assumed that PAN card is actually transaction card because it's involved with financial transaction.

E: So, I counted three questions.

Firstly how do you audit governments and again the European Union consists of 28 member states. They have varying levels of administrative advanceness. Some of them are extremely administratively disorganized I assume. Others have more stable institutions that act very predictably. The Scandinavian countries for instance have for a large number of hundred years been developing practically without war or conflict. Their public institutions work very well, has a very strong transparency principle. If you wanted to follow electronically or on paper or otherwise, the functions of the government in Sweden, you more or less could. There are some fishy maneuvers that they are doing with the budget to make them less transparent than they could be but this is all a kind of a political game. It's about the amount of time that you're willing to spend deciphering how the government is covering up cutbacks.

Now the European Union as an institution, as an organization of member states is closer to the Scandinavian model of transparency than it is to say, the level of transparency in the UK or in some of the administratively more disorganized communities. But there is a lot of work – so, in particularly Eastern Europe there is a lot of work going on in anti corruption because this is seen as a very important part of their development into democracies. The UK is weird for me because they have the opposite assumption as Sweden. So, everything is assumed to be secret unless there is no reason for it to be whereas in Sweden we would define that everything is public unless it isn't, unless there is a strong reason for it not to be. So, earlier this year I won a law suit against the law, the chief of the law enforcement department to get access to his cookies and web history, like web cookies. So, I'm expecting to get a letter any week now with a full print out of all of the cookies stored in his device between June 2015 and February 2016. And you could get that kind of random data also machinery

doubts, reports about hardware crashes everything for which the government doesn't have a reason to classify is not classified.

Your other questions are about private contract law in the bank sector and how if you've been wronged can you demonstrate this much to court. This is not a trivial issue at all. Consumer protection authorities have largely not cared about digitalization or enforce the normal practices of consumer contracts in Europe. Normally in European contract law with consumers, the idea is you have very simply contracts with consumers that are easy to understand. And this has been developed through consumer rights protection acts in 1970s and '80s. We don't – because the European law is civil law, it's not common law, so, basically any conflict that can arise has to have been predefined by the legislatorial way that also allows for contracts to be quite simply formulated. Now, in the digital space it's often the case that we borrow from American contract law where their law end user license agreements are common or disclaimers such as, we try to give you state of the art security but if we can't do it then, you know, it sucks to be you and you can find us in a court in California. So, the Norwegian consumer council launched just a month ago a case in court against apps on mobile phones for having difficult to understand and un-maneuverable privacy agreements. This is to my knowledge – no actually so, the German consumer protection agency has also been active in trying to get the rights of users to say, sell computer games second in electronic environments or I think they failed with that one and they've done some other stuffs as well like a few years ago which were very interesting. But normally the consumer protection authorities just haven't cared and now the contract situation is out of control. And certainly for banks it's a very peculiar situation. When we were negotiating the general data protection regulation in Brussels, the bank northeast of Europe would come to the legislator of Brussels and say, we can't give the user data of our customers because they are our intellectual property.

While they were unsuccessful in getting a specific provision in the regulation that says that they don't have to share the user data because of their own intellectual property interest. There is still phrasing in the regulation which protects trade secrets or intellectual property as if the personal data of a person of somebody, an individual, me, could belong to somebody else just because I've had to give it to a company to – for them to provide me services. So, again, this was already there in the data

protection directive from ’95. In ’95 the wording was slightly stronger such as the industrial interests must not or – no, so, the data protection interests must not interfere with industrial interests. In the general data protection regulation it says, should not. So, hopefully there will be some form of litigation in the future where it’s clarified whether should not means that effectively there is a blanket ban for individuals to request this kind of data from banks. But again we will have to wait until after the regulation enters to effect and some industrious individual takes it to court in one of the member states because until then we don’t know.

It is a problem in the banking sector and any kind of sector that uses electronic signatures in Europe that the legislator unwisely and against my recommendations decided that the liability for transactions conducted with other electronic signatures should rest fully with the consumers. So, the consumer has the burden of proof. But in fact you cannot then access the proof that you need to win against a financial institution or some other company because any kind of information you would need to proof that you’ve been wronged would require you to undertake some form of computer misuse because they will not share their logs with you voluntarily. They can evoke trade secret laws, they can also invoke computer misuse acts. So, as a consumer you are very, very vulnerable. But I’m happy to say that the Swedish consumer authority in the report that was released also just in the last month seems to direct a bit of attention to this issue at least saying that some further studying should be done on the issue. And I’ve raised this extensively with the government over the last couple of years in Sweden arguing that we need to advance beyond the European [Inaudible 3:13] and provide a stronger protection for consumers. But it’s going to be a long way ahead and the banking lobby is very strong and employ a lot of people and they are extremely important for a lot of other parts of the economy. So, if they’re very intent on keeping their liability exemptions that could be a – that is a formidable challenge to get the political system aboard with that.

One of the ideas I had was because law enforcement wants to start hacking people now in Sweden and many other European countries. So, that means law enforcement wants to take technical security away from consumers normally. So, I’m trying to formulate a problem for the legislator wherein, law enforcement can only hack people if people are not completely reliant upon the technical security of a system, which, if the liability falls on them by law when the technical system malfunctions, clearly they

are. The technical system is the only thing that stands between them and losing their money or losing process or some contracts or suffering harm. And then my idea is that, law enforcement will want to hack stuff so much that they will be able to pick the fight with the banks on my behalf. But it remains to be seen if this is a successful strategy and you'll have to wait for further reports on this. Thank you.

Q: Just a quick follow up on that. How will you view whistle blower information then in a privacy context?

E: Yeah, so, Sweden has – again, this depends between the different member states. Normally the way that whistle blower protection works is that the journalist may keep their source a secret if they want. In Sweden there is a reverse secrecy. So, the source can request anonymity and the journalist has an obligation to keep it. Now the intelligence agency of course monitors all of the communications regardless of with whom. So, there has been this controversy whether the intelligence agency is getting source information or not but they assure us that they have implemented a technical system which does not let that sort out source information when it's appropriate. So, one could either say that we have a very strong whistle blower protection in the law but in practice, at least the government for issues of national security could quite easily circumvent it. That said, in most European countries unlike in the US, you run no risk of getting sent to jail for 50 years. Most European countries have considerably more measured jail sentences and you'll be looking at, in Sweden I guess, six months up to a year. And certainly if you leak something that was considered very relevant for the national discourse and you were a government employee, that would be a tough sell for the politicians to justify such a case.

The worst situation is really in private companies. So, how do you deal with whistle blowers from private companies? And there we're seeing now an onslaught of trade secret legislation which is partially emboldened by a European initiative that passed only last year and is now being implemented in the member states. And that's going to make things tougher for employees that discover uneven activities in their work place. It's also going to mean lot of other problems for labor law incidentally. So, there is still a lot of work to be done for people that work in large institutions that aren't public but they'd still feel that their company or their working place should uphold some form of ethical standards which they are currently not upholding.

F: To answer your question, PAN card was 1.0, it was, even though we use it for the transaction, nobody would actually prohibit you from doing the transaction. It's just getting logged alongside the transaction whereas AADHAAR actually prohibits you from the transaction based on rules. So, you can actually have – it's not there today, this is where we talked about the exclusion. So, it is theoretically possible that either you can be rationed cigarettes or liquor so, thereby you are actually, you are physically transacting. While transaction AADHAAR acts, could act as a gatekeeper. And an extension of it would it like, tomorrow when transactions are automated, like you could have recurring bill payments. Something like this could also be failing.

Q: Just to add to that answer, the other key way in which this passive to active digital ID shift happens is that the PAN cards or the passports for example, these are documents that give – see if you are producing these documents, it tells the other person what is written in the document itself. Whereas the information that AADHAAR possess or the AADHAAR card, which is not a real thing, possess, is not in the card itself. It's kept somewhere else hence this need for this real time connectedness of the card and the number. And the number allows the other person to which you are giving the number to learn something about you which is not necessarily written in letters, in legible letters, the document itself. And that is where the KYC bit, the payment authorization bit and various other kind of service authorization in general comes in where the card is just is not a card. It's a number and once you've given that number and you have given some other, further information, it allows you to do certain actions on behalf of yourself.

Q: Hi, I just had a question building on the exclusion issue surrounding ID. I don't think what's talked to – I mean there's people who know far more about India than I do as I've been only here just over 24 hours. But I think we could recognize that when you introduce an ID system thing you're actually talking about the fundamental ideas surrounding [Inaudible 9:36], the nation and the state basically in many countries as you have. For example, people live on borderlands, maybe migrant populations who move around, populations who have moved in from abroad, from other countries maybe still identify they are such by others or themselves. With ID scheme you are saying, this person either is definitely a member of this nation or isn't. Many identities are more complicated than that. So, it's a fundamental, political question as well for debates, who is Indian, who is Canadian, who is British, a fundamental kind of political

questions which avoided often when an ID system is introduced as purely, yeah, we're just going to help you out to make things more convenient or easy to use. So, I'm wondering how this is playing out in the Indian context?

A: I think let's have a couple of questions together and then answer.

Q: Okay. Actually my question is extremely related. Because you've brought out this, you mentioned something about anti discriminatory frameworks and red lining issues that are being tackled in EU. And we've seen this historically also in the US case where you've either had excessive disclosure of data has either been discriminatory or predatory especially in financial services. How do you see supervisory structures working towards eliminating these at least in the private sector and especially in the financial side because we've seen a lot of these happen even in India? Certain, very prominent public, private sector banks don't lend to certain areas. It's not whether you are particularly Hindu, Muslim or a Christian. Yes, if you are from a particular PIN code, you are not given a loan. And these are called, do not track areas, these exists. We've been talking about anti discriminatory at work red lining across western countries, across eastern countries but never really has there been an action across supervisors and supervisory structures to negate this. So, at least in the EU you see this working out and you have an active anti redlining strategy at least for the financial sector. And I know you said the lobby is hard but is there anything happening here?

Q: Hi. For F, I just wanted to know and you've touched upon this but I just wanted to know if we can use the historically created legislation on data theft for maybe safe guarding the rights of the data subject? Because if we have a way of putting liability on either government or the private companies, and maybe have a sequence of compensation for them when there is either. So, looking at data but from a perspective of theory in that sense. Is there anything possible on that?

Q: F, what would be a shadow stack? Can you just explain a little? And how will it be implemented? And just to follow up on it, will it go towards actually supporting the AADHAAR database by itself?

F: So, first to answer whether ID gives a political identity or not. As I said, I am ID novice but I think AADHAAR escapes that question. AADHAAR says that, AADHAAR can

be caught by anybody who is in India for convenience. Be anybody else who is better knowledgeable of AADHAAR can answer that question.

Q: So, this – it's been a deliberate, it's been a decision not to make the UID relatable to nationality, to citizenship. And it's interesting because when this whole thing was first started, there were various ways in which, various avatars it took. So, in the first round you're saying that Pakistanis are a problem and there's infiltration and therefore we need something along the borders and we need to have some kind of a card which will quickly help identify whether the person is Indian or not. Then, between then and the time that the national citizenship, the citizenship act was changed, it shifted from the Pakistani to the Bangladeshi who became the illegal migrant and therefore it was the illegal migrant who was our problem. By 2006 it shifted to corruption – no, it shifted to targeting beneficiaries. So, you needed to know the people so that you would know who to target to take, to deliver services to. By 2009 that became corruption.

So, actually this is not a project that has, like I said, it is not telling us what it is about. By now it is clear that they are not talking citizenship, they are talking customer. Actually it's a very clear statement has been made now. So, it's got yet when the questions come up they will say there was this Pakistani terrorist who was found with an AADHAAR card on his body. So, then it becomes like, how does he get an AADHAAR card? So, it's not only that it is deliberately come to this point, it's also that we've all been deliberately kept in a state of un-understanding about this. So, we don't know whether it's mandatory or not, we don't know if it's for resident citizen, we don't know what we're supposed to give or not. So, there's an obscurity that is meant to allow for many wrongs.

Q: '99 is Pakistan, 2003 is Bangladesh, 2006 is targeted beneficiary, 2009 is corruption and then rubbish.

E: So, I don't if this strikes anyone as interesting, most of the, a lot of the European governments of course have central ID databases, the UK being a notable exception and Ireland. But they came about in times of war. Normally they were introduced in the Second World War ending, then they just kind of stuck around. So, it strikes me that it's kind of interesting that India, which has I mean some nominal border skirmishes that don't matter so much but it's certainly not the kind of disaster that was the Second World War on Europe. And you're having this introduction of a

national ID system in a completely different political context and that will be extremely interesting to evaluate in 10, 20 or 30 years. I would have thought, it's just an observation from an outsider.

Now, for the question in the back that was raised, I'm not sure that I understood the super structures. Supervising? How do you supervise? Well I mean, so, this is like the fundamental challenge. Like I said that the DPA in Sweden is under resourced. There is not much coordination between public authorities unless the politicians specifically tell them to. The European Union certainly doesn't have the powers to intervene in member state governance structures. And there is one particular law in Europe which relates to personal data protection electronic communication efforts where the member states have solved the supervision issues so disparately that the law effectively hasn't been enforced at all. And I speak of course of the e-privacy directive and the cookie legislation that nominally provides a protection against arbitrary tracking by online actors when you surf the web. But in practice it hasn't done anything at all.

So, supervising is a problem. And enforcement of the legislation is also a problem. Even if you have a designated public authority, you can't be certain that it will do its job. In Europe as opposed to in the US, it's often a problem that individuals can't claim their own rights in courts. So, I read about one case in Sweden where a lady won against the government for mistreating her data but she ran up to €130,000 deficit because she was also ordered by the court to pay the trial fees for the government. So, even though she won her case and she was awarded civil damages, she still ran at a very high personal cost. So, that's a very good incentive for individuals not to claim their rights. There again, I think you will need a combination somehow of the American and European systems where you have regulatory authorities that can represent a common interests and that are adequately financed but something a lot of European countries should think about is can we introduce class action suits? This is being reflected upon in some of the member states. Can we raise civil damages?

And again, I would think the UK is kind of an exception to the rest of Europe in this case because of the common law system in place there but certainly for continental Europe or the Scandinavian countries, we need to give individuals separate tools to exercise their rights exactly in those cases where the public authorities do not. On data theft law, I have a very disturbed relationship with data theft as a – the way that it's

manifested itself in Swedish law or in European law or for instance in the cyber crime convention. Because normally these laws are tailored to protect the owners of computer systems but when you talk about data being forcefully removed from a system, then actually the interest of protection in that law, the legal object of protection is the government or the company. So, it could be – the first Swedish data theft law which was concurrent with the data protection act of 1973 states that the government has an interest in knowing what is in their databases and knowing that this is correct. And therefore we will make it a crime to unlawfully manipulate access, copy or whatever to data but it's protecting the government. It's not for the interest of the individual to have their government know relevant and adequate information about them, it's to protect the right of the government to know what's in their databases.

So, the data protection framework somehow cleverly works around that by clearly putting the individual at the center which is also something we have from the German constitutional court in 1983 that we need a legislative framework that makes the legal object of protection the individual. We need a better consumer rights framework for ensuring that the individual is protected. And if I could choose I would just scrap these computer misuse acts and not at all try to criminalize. I mean this is of course a politically unrealistic proposal but not at all criminalize using personal data that belongs normally to the person as a way to allow the government to prosecute people from messing up their databases and instead you should focus the criminal law protection or the theft laws in those cases on what was the actual harm that was enforced by such a misuse happening which used to be the case in Spain until 2010 and then they changed the law sadly after visa was endorsed.

F: Okay, on shadow stack upper – it's necessary for us to do both. Like one is, participate within the system and build utilities which will increase the rights or give back rights of people. This is like building an anti cookie add on for Internet Explorer even though you might not believe in Internet Explorers, the open model and the proprietary nature of it. It is essential for us to build that cookie blocking software for internet explorer as well. On the other side we could also go ahead and build a full blown stack that is completely independent of this but it solves the problems that India stack solves. So, similar problems but with the values that we care about and that is more democratic so, the – we take the pitfalls of the existing stack and build a

newer stack completely independent of it. But it's going to take a long time, maybe that's – but that's how probably Linux started. Nobody used Linux for 20 years seriously.

And the first demand would be the open access to the existing infrastructure. So, if there is UPI, API that is out there, I should build the Firefox app of it. You could build the Internet Explorer, you could build the Chrome, you could build million other browsers but I will build a free and open software on top of the existing stack. That is one. But we should also see how we can entirely evade from the stack and build a completely parallel stack. There's a lot of work.

A: With that lovely note and lovely work plan ahead, let's move to the next question. If you have questions please keep them to yourselves we'll come back to you. We'll have a few minutes of discussion then we will go for lunch.

Session 4: Digital Money and Financial Inclusion

G: Okay. So, I am going to talk a bit about financial inclusion. So, I think we are in a country where 94.7% of the villages are actually unbanked today. There are no bank branches, there are no banks in 94.7% according to the RBI's own figures, Reserve Bank of India's own figures. So, it's been debated for a long time that these people have to be included as also the so called urban poor need to be included into the mainstream of the financial system and they somehow need to be banking which means the need to make deposits into banks and they be advance some kind of credit. So, this has been the story which has been sold in India by the Fintech sector for some time to build up to the theme that the Fintech sector has today. So, I am going to trace very quickly the history of how the story line has been built up.

So, sometime in 2008 December, we had a company, non government not for profit section 25 company which was created called the, National Payments Corporation of India. In January 2009 we had a government body, an autonomous government body created as a division of the planning commission of India where an executive order called as the UIDAI, Unique Identification Authority of India. It's interesting at almost the same time the United Kingdom was crapping its program on the national ID. And Cameron who had become the prime minister had during his tenure, as the leader of the opposition had promised that he will get rid of the UID, the national ID program in

the UK and which he did after he became the prime minister. And at the same time India was talking about scaling up this identification number for everybody.

When the UID was created it started lobbing with the Reserve Bank of India almost instantly and putting pressure on them saying that, we are creating this thing called as the AADHAAR number or the UID number and this should be used as a basis to allow anybody in the country to open a bank account. So, it should serve as the basis for doing a KYC. And it's evident from the records with the Reserve Bank of India that the Reserve Bank of India resisted and it said that, firstly this is not in accordance with the extent guidelines that we have been following. It's not in accordance with the BASAL standards for keeping your customer's records and it's against the prevention of money laundering act which is in force. And therefore a practice of using this number in order to open a bank account or do a KYC is unacceptable. With a lot more pressure from the UIDAI, finally in January 2011, the Reserve Bank of India succumbed and issued a circular to all banks saying that, they may accept the AADHAAR number or a document of AADHAAR enrolment as a KYC document on the basis of which you can open a small bank account which will be subject to the PMLA, Prevention of Money Laundering Act. And this PMLA required that this small bank account has to be opened in the physical presence of the branch manager and whoever is opening it has to be audited, cannot have more than I think Rs. 4lac and has to be closed down within three years.

So, there are a whole lot of restrictions which are placed on this small bank account. So, the Reserve Bank of India's logic behind saying this was that, look the government of India has been concerned about even the introducer scheme which allows us to open bank accounts by people introducing new account holders because of terrorism and money laundering. And we have placed accounts which come under that kind of a category as small bank accounts so that they can be closely monitored. So, there is no reason for us to treat this any differently. Now the UIDAI as recorded in documents actually can be seen, it was not satisfied. It was annoyed. So, the pressure went up on the Reserve Bank of India. Finally what the Reserve Bank of India did was it said, well the custodian of the prevention of money laundering act is the department of revenue in the ministry of finance. So, let them actually take a call. And the entire thing went up to the department of revenue and the department of revenue conducted a meeting in Delhi, here, with the UIDAI representatives, representatives from private banks and

some representatives from the Reserve Bank of India. There are two sets of minutes which emerged. One from the RBI which actually indicate that the RBI put up a spirited defense and said that, look, this is something which is not going to work. And the department of revenue which actually said that, look, we have not put any restrictions on using the AADHAAR as an officially valid document. Why are you placing any restriction?

So, in September 2011, the Reserve Bank of India actually issued a new notification saying that whatever we had issued in January Para 5 of that stands cancelled. Para 5 was actually placing restrictions of AADHAAR, accounts opened with AADHAAR having the restriction of PMLA based small bank accounts. So, they did not even say it in a very direct way, they said it very indirectly. The second thing that the UIDAI had been pressing on was the use of AADHAAR e-KYC, electronic KYC instead of actually physically have a document. They said that if there are AADHAAR numbers which are queried on our database and you get back the information and you see that to open accounts, that should be acceptable as a KYC. Interestingly the e-KYC norms of the UIDAI indicate that e-KYC records returned from the UIDAI will be stored by the bank for at least six months for audit purposes. Now, at least six months basically means that, you know, no audit as you know ever takes place in six months anywhere in the world. It usually is, audit is a delayed process. So, in six months actually banks can get rid of whatever they got from the UIDAI, purportedly got rid from the UIDAI and there are no more records of the customer as where did this customer come from? Who is this customer? So, therefore you can actually create a ghost customer, an anonymous customer, a fraudulent customer, multiple customers all permutations combinations because you don’t have to say who the customer is. The customer can't be audited anymore.

Now, the whole premise of using the UID number in the first place was that UID number is a valid individual. And if you really ask the question, how can you define what the UID number is? The UID number is simply a 12 digit number which the UIDAI assigns to demography and biometric information submitted by private parties and none of this information has ever been verified or audited. So, therefore we have no clue whether even the one billion purported UID numbers correspond to a real individual. Whether their addresses actually exists, how much of this is ghost individual, how much of this is actually duplicate individuals. Nobody has ever verified

this. Nobody has ever audited this. The entire process of identification of individuals does not exist in the UIDAI's enrolment process.

If you look at the UIDAI's enrolment process, it verifies documents. It does not identify individuals when collecting demographic information. So, therefore there is no reason to believe that any UID number is anymore valid than any other number that you can use. Now, if you see the entire functional creep of this UID number across all our Indian public and private databases, is therefore actually jeopardizing governability and the financial institutions themselves. So, while all of this was happening, simultaneously the UIDAI had signed up a memorandum of understanding with the National Payments Corporation of India. Not with the Reserve Bank of India but with the National Payments Corporation of India to create an AADHAAR based payment system. Now this AADHAAR based payment system interestingly is one which is replacing the Reserve Bank of India's or the Government of India's own NEFT which allows you to electronically transfer money from account to another account. What does the AADHAAR based payment system do? It says that you can transfer money from one AADHAAR number to another. Who runs it? A private company, not the Government of India, the National Payments Corporation of India. How does it run? They actually say that you can associate your AADHAAR number with n number of bank accounts. However the National Payments Corporation of India keeps swatted calls as a mapper which is a table which maintains a record of which is the last account that you have associated with the AADHAAR number.

So, I can go and associate my account, let us say in Bank of India with my AADHAAR number. I can actually have a money transfer come in from let's say a subsidy or from a money transfer from another AADHAAR account and then subsequently I de-link this and actually overwrite this record with by linking my account in State Bank of India to this AADHAAR number. So, the minute I do that the NPCI's mapper has no way to tell where the money came from and where the money went because it overwrites the record in the mapper. They have no logs of this maintained for security reasons they say. So, there is no way to trace how money transfers are done anymore. So, therefore it becomes extremely easy as you see to do transfers which a banker would call as, money laundering. A banker will call as a, Hawala transaction. A banker will call as, ensuring that I can siphon off money or pass black money. Now, on the one hand we have created a framework where we have possibly more than 16% ghost individuals,

residence in India. On the other hand we have created a mechanism to create bank accounts with these numbers. And on the next step we created a mechanism to transfer money from one of these to another of these in a way which can't be traced and which will not be reported because nobody will see the difference, nobody will actually know what is happening.

Interestingly we had this scenario, we have this scenario we are all facing whereby all of us who probably credit cards or debit cards and mobile phones when Rs. 500 and 1000 are demonetized or taken out of circulation, we have been facing hardships. Imagine the plight of those people who are not even having a credit card, debit card, mobile phones or any of these devices to bank. They are all facing a serious issue in terms of how do you deal with this scenario? In this context, if you were to look at what's really happened in the banks, yesterday news channels were reporting that there is a 1 to 5% increase in deposits in the last quarter over the previous three quarters. Now, they were asking the question, did some people actually have knowledge about this removal of Rs. 500 and 1000 and did they actually park their money in small bank accounts in different banks? Because they didn't present data about one bank but they presented data from several banks in terms of increase of deposits. Now, clearly if you look at this kind of a scenario, one asks the question, how does one ensure that the banking system remains auditable? How do you ensure that by giving us maybe a privacy law, they don't actually wrap this up from our eyesight, from our ability to probe and our ability to question and say that, look, this data can't be made available to you? That you can't actually trace whether these AADHAAR accounts are genuine or fake. That you cannot trace whether this transaction happened from account A to account B. Where has it gone?

If you are not able to actually have some mechanism to examine and check this, we will be in no position to ensure that the banking and financial system of India can stand the test of time. This is an issue which is an emergency issue. It's an issue of national security because I think we see on the one hand if the prime minister says that it is because of national security and in order to ensure corruption is wiped out and for this moment of integrity that I am getting rid of Rs. 500 and 1000 accounts, why is it that we are not getting rid of AADHAAR based banking? Why is it that we are allowing 'benami' accounts to be created? Or a number which has not been audited, it's just a number. The UIDAI it doesn't even certify identity or address. It doesn't

certify anything. How can you allow it to be linked to financial inclusion? So, I think you probably have lots of questions and I don't want to take away time from H who probably wants to present different side of the story. So, I'll stop here.

H: I must apologize to C, I might sound like a digital payment evangelist. So, anyway there are some quick number Boston Consulting Group says, India's digital payment will grow to $500 billion by 2020. So, looking at 15% of the GDP that is going to be on digital payments. I mean whether we agree or disagree, seemingly disagree, this is happening. So, I guess what we, our conversation should be about how we can make it better because the government has been pushing it and pushing it through various means, covert, overt whatever, it's happening. So, the first one of course which has been discussed quite a bit is JAM Trinity. Within that is something called Direct Benefits Transfer which I work on, which is, how do you convert government programs increasingly which has been touched upon to digital payments. And this comes in various forms. There is an interestingly acronym BAPU which is, Biometric Authentication Physical Update.

If you go to your ration shop you authenticate yourself and your entitlement pops up on a pause or whatever screen that's available and then you are given your entitlement and you give the government whatever you owe, the Rs. 40, 45 which you've always been doing. This has been tried in Andhra Pradesh and Tamil Nadu two states where most experiments work and they've been doing well. We've heard stories from Rajasthan where AADHAAR has not worked, there have been major authentication failures. In my experience AADHAAR fails. About 20% of the time it doesn't work. And that's made better with iris scanners which improve that to maybe 10% failure but that's pretty significant. The government has done this obviously in LPG which is a largely urban scheme. You would enroll your AADHAAR number, you get your subsidies in your account which is the other way of doing it which is direct cash transfer which is also being experimented on somewhat sensitive schemes like the PDS. And they've tried, the PDS converting into cash in Puducherry and Chandigarh where the response has been very mixed both urban areas with high levels of exclusions both because of access to banking, access to market, banking habits and AADHAAR authentication failure.

So, this is how the government is thinking about it and I'm working on experiments on kerosene which is being scrapped over the course of the next two years. They don't

want to see kerosene anymore. MGNREGA wages have already gone to direct transfers, fertilizers which is going to be the next big one which is about 75000crore worth of subsidies, 65% leakages according to the economic survey. So, all of this is going to go on. But it's interesting to see JAM and unbundle it a little bit because despite the huge push of PMJDY, we're still at 53% bank accounts per individuals. They claim 99% for all households and 100% in some places but when you look at individual bank accounts they probably duplicated it in many, many households and individual bank accounts are 53%, 43% for women which is abysmally low which means women's work, women's wages is still not being counted in the formal channel. The second one is AADHAAR, it's about 80% but from what I gather can't be trusted as a number. I don't have one, you don't have one. And then finally is Smartphone, 20, 25% mobile phone, feature phone is about a little more but I mean, again, duplication it's about 1 billion phones in India. But again, we don't know how many phones each individual has, property dealer seem to have five.

Even my observations in terms of what I've seen is that World Bank says, as of 2014 India had 43% so, if you had 53% of all individuals who have accounts, 43% are dormant, as in, have not been used in the last year. I have been across maybe five or seven states in the last one and a half years looking specifically at use of JDY accounts, my sense is no one is using their Modi wale accounts, which is what they are called, Modi's accounts. And people who had accounts are using them and have been for the last two or three or four years. The ones who didn't have just this one account. So, the government's push and we've read the Indian Express report on Rs. 1 bank balance which have reduced the no balance accounts as well, which I would believe because, like I said, usage is very, very limited. So, I mean the reason I have rattled off these numbers is not only [Inaudible 12:55] but just to say that the digital financial inclusion has been pushed by the government through this JAM and JAM adds this silver bullet to all our issues and moving government schemes to this platform is all a bit premature and I mean to the point of, what is demonetization meant in the last few days for people who don't have access to these digital platforms.

And the way to think about exclusion and how our data is used or not used is really important because people are, I was just saying that my experience has been and that's why I've been a digital payment evangelist is because I have been looking at it from a social security perspective which is that, I did my first experiment with

payments on basic income in 2010 where I found that access to a bank account in the name of a woman meant absolutely wonderful things for her within the household, within the community and access to money. But I also understand that because it is being so rapidly digitized and we don't have the time to actually onboard people onto these platforms, give them the information, the awareness and create safe systems for them, that means a lot of people are also getting left behind. I have been evaluating a PDS experiment in Bangalore, a city that I think a lot of you belong to, where I was telling the food secretary, I have not been to a single ration shop where I have not had people burst into tears because these are extremely emotive things. And when you can't access 5kilos of rice that you are entitles to because your AADHAAR is not working, because you got a cataract operation and it didn't – your iris is gone and these – the major people who suffer are old people, people without any access to, you know, illiterate people. No access, no information and these, this sort of rush of the systems needs to examined a little bit closely.

Beyond JAM there's obviously India stack which has been discussed, there's UPI but what is also more interesting and has not come up is something called, SER1 which is also server for all which is an interface that, and I quote the government, an interface for beneficiaries and their providers to deliver public benefits in a rational objective, convenient and [Inaudible 15:22] way. Ser1 is going to be a centralized database. The unit of analysis is now going to be the household which means that all our AADHAAR numbers will get aggregated to a household ID so that the government is able to give because benefits exist both at the individual and at the household level exist for – and it's so easier. And again, there's a rush. So, all ministries and all state governments have been asked to onboard onto this Ser1 platform by March 2017 which is absolutely no time because all of this while state governments have been making their own servers and own databases but now they've all been asked to move to this unified centralized database which is going to have information on every individual, every scheme that this individual is entitled to, household entitlements for food, for fuel, for fertilizer, for whatever else and it's all going to be in one place.

The idea is, from what I understand is that, the government wants to be more proactive in its governance which means that if you have a new born baby who is due some immunization they want to be able to send you a text message to say, hey you need to go to your local ICDS center or wherever else. So, that's what the government

imagines it being and so, I mean, so, indeed the data visualization of this is where, there is this massive thing and it sends a little note to your friendly ministry woman and child development and when they will send you a text. So, it's all going to be managed in one go. Now I have seen AADHAAR authentication happen in real time and what the government says will take two to three minutes, it actually takes 15-20 per transaction on a good day. So, why we're trying to onboard information on the servers where we don't have the bandwidth for, it's again a scary proposition because I have seen so many experiments being including the fertilizer experiment that I will touch upon and – but again coming back to why I believe that digital payment is good is because leakages I think are you know, it's going to be [Inaudible 0:18] or whatever 45% leakages on PDS, 45% in [Inaudible 0:22], 65% in fertilizer so, [Inaudible 0:26] subsidy programs and again I know that where bank accounts work with there is access to banking it is – it works it happens.

I know that Tamil Nadu and Andhra Pradesh have done very well on the PDS. There is no transaction cost I know the government has been claiming 22000 crores or 32000 crores which even Arvind Subramanian, the chief economic adviser has contested but there have been savings which if we overlook the exclusion of beneficiaries and then access to credits which I think is an important one because there is a 15 Lac crores deficit in the market for MSME credit, these small traders are on a 15% of women entrepreneurs get formalized credit. So, this is something the transaction is freeze, the documentation all of that can help but again I understand that we have to make them safer.

Now there is also so why this push is happening, the response that I've seen is unclear from the people it's meant for. There is a general trust deficit when it comes to the government; they are not comfortable with technology, banking systems etcetera and there is a greater sort of cause of fear that is happening so for instance I just was in Krishna District where we were doing AADHAAR BAPU for fertilizer and – and then the farmers suddenly realized that AADHAAR was now being seeded with – of their bank accounts, their mobile phones, their land records, their children education, attendance in many places, any benefit that you'll get from the government now AADHAAR is your sort of password for it and be as part of the government advisory were cornered to ask why the government needs to know how many banks I'm using, how much land I have so, there is again a little bit scary is again the speed at which

digital payment is happening in government schemes particularly. The systems have not been designed very well. I see servers fail all the time. I'm not sure, I'm not a technical person but I don't understand how the backend works, the leeway time for authentication is very much and the other thing which is actually the most scary which I saw in Bangalore is that, Bangalore One Center which is a public private partnership actually have the authority to change data which means that if you want to add a beneficiary onto your PDS, remove a beneficiary on your PDS, you can get a login quite easily. The food inspectors login or whatever someone's login is available for you to change government databases which is a really scary possibility especially when it comes to your entitlements like food.

The other thing that I found actually quite rampant is, how the privacy for the poor is not regarded as important. So, again, I don't know and IC is probably designing these systems for all these digital on boarding so, a seed experiment is happening for seed subsidy which is a very small 180crore subsidy that is being digitized in UP. All the AADHAAR numbers for all the farmers are all available in this again, easy to access login page. All you need is some sort of government ID which I got because I asked nicely. So, yeah and then when you ask them it's actually not right because the government says, AADHAAR number should not be in full form anywhere. They say, *ki nahi ye kya bechara kisan hai*, you know, this is a poor farmer what does he have to hide? And we are here to help him. So, that idea of privacy it doesn't exist even in the minds of government officers who may not have anything particularly – I mean they're not conspiring anything but they just don't understand and value. So, I guess I've been thinking about what to do as we go ahead and because like I said, digital payments is happening, the government is going for it. There are like 11 panels in every ministry looking to onboard you in some software, some server, some payment platform. So, I think that the thing to me that is important is to first of all make the people aware who are actually – because you can't get a benefit in this country without AADHAAR. You can't get a divorce with AADHAAR. Like I mean it's really becoming problematic.

So, at this point you need to make sure that people know where – that, a – your data is being collected, b – where it's going, what it's being used for. And to your point, let's make it commercially viable for them to share their date because I think it's – transaction histories for credit, let's do that. Capital Float is doing it, a bunch of other people are doing it. We might as well make it economically viable for people to share

their data and in their knowledge. And the second thing is I think just a massive sensitization of what it means to share data for just the government even because like I said, you move to Barabanki district of UP like nobody knows privacy. That doesn't exist as a concept, it's not self reflexive enough. So, I think that that's where I'm at, yeah. Thank you.

A: We have 10 minutes for discussions so, all yours.

C: First I'm not going to discuss this but I want to start with saying that I have a great deal of unease with this statement and endorsement of why don't we just – if someone is going to make money on it why don't we also make some money on it because it's our data? I think, what are we forgetting in all of this? I mean who's going to be giving this consent? Whose data? What kind of people? Can they really do this? And, who are being made the subjects of this exercise? I think it's a very dangerous way to go. Sometimes you ask the wrong question you come up with the wrong answer so I think we really need to be careful. I am just wondering why you thought I would, I mean you've actually provided all the arsenal for what I've been saying so why would I disagree with any of this? But I just had something, one is this idea of I don't know, I mean I have to go back and check what the actual definition of a nanny state is. But are we endorsing this idea that a nanny state is a good thing? A paternalistic state let's say is a good thing and that's what they are projecting themselves as being. I wondered where you got that figure of 45% of PDS being whatever is from because when the NITFP did its study, not its study, did a paper, it found that it did not – it actually said that we are assuming this, we are assuming that and we are assuming the other because they did not have any data. And they were saying that, when Reetika Khera questioned them on this saying that, what are these? I mean these are not even estimates.

They said, yeah, yeah these are only assumptions we are making because there is nothing. Now in 2005, 2006 there was a huge food rights activist, came up with this saying that, listen we are having a major problem with leakage in the system. Leakage in the system was not coming from the people who are taking rations. It was coming at other points. What you have addressed through this is people who are taking rations. And if you look at what happened between 2006 and 2010, the systems had already changed in multiple ways where in fact in many places these so called ghost beneficiaries were not more than 2%, where the leakage perhaps had been brought

down to between 10 and 20%. Now we've reintroduced through the UID, we've reintroduced the exclusion of a certain amount and fraud of another amount. You go to Rajasthan you'll not only see exclusion you'd also see fraud. So, one I'm wondering where you got that 45% from, if you could just note it in a sense. And that that these are changing figures which have come because people got control and got into the act themselves. They are not subjects of the state. They are not there waiting for the state to make all the – and the corruption in the past 15 years have been huge between the state and corporations. All the scams have been about corporations and about the state. And what we are saying through this process is, let's hand it over to them to reduce corruption. There's an absurdity in that which I don't know how we cannot see. So, that's one.

And the other is, I just wonder has there been any kind of estimate of what is the cost of this exercise? Who is paying the cost? Where is it being recovered from? What is anticipated? MKSS tells us that they run a ration shop, they had to buy point of service device for Rs. 18000. It went 'fat' within three months. They had to give it for repair. When it came back after it was repaired it was all fine, the screen was not black, it was fine again but it wouldn't work because they said, till you pay us the Rs. 18000 again we will not activate it. So, are we aware, I mean it's not governmental cost, it's the cost that you are putting in multiple places. Who is paying these costs and who is benefitting from this? Or does this matter at all?

Q: Okay, so, my question was on the NPCI and you were referring to NPCI as a private body because from what I gather the stakeholders are, 60% of them are public sector banks and there are only four private banks as stakeholders. And the board is basically one nominee from each of the promoters as well as a nominee of the RBI. So, why would, why are we classifying this as a private sector entity? Just because it's a corporation? It's a company? Or is there something else which general documents don't show?

Q: I have this question basically regarding the integrity of AADHAAR, the point of the first speaker is. So, essentially the larger argument being that AADHAAR is just a series of numbers and so – from whatever I understand of it, AADHAAR basically what it does is, it authenticates who you are you say you are. So, there is a biometric part to it, subject to the failure 20% approximately because the cornea detection goes and the thumb print detection goes. For a lot of people who engage in activities which wears

off your fingers and all. But if you can look at as an incremental of between – so solving the question of representation basically saying that, this is an incrementally better way of representation. So, if you have a card and you turn up with a card, there is no systemic way of authenticating a few other person who's turned up with a card. And AADHAAR largely if you look at what it stores as database, it just stores those that information authenticates that. It doesn't – so, it doesn't, the servers don't really store anything else beyond the biometric and your cornea footprints. So, I mean basically what is happening is, it is an incrementally so to say, a better form of just mapping the person to the document. It's not really the document. And that is how it's being used is my understanding of it so just want some clarification on that.

Q: I have two questions, one for G. You were mentioning that NCPI overwrites the account number and there is no auditability. How is this even – are RBI or international agencies – this is against basic banking norms. It sounds very scary. So, how is this not being looked by anyone else and are they willfully ignorant of this? That's one. Second question to H, you have mentioned Tamil Nadu being a successful state. What are the measures and how do you classify that? Because Tamil Nadu has largely been a PDS friendly state and ever since that happened in 2004, the PDS system has vastly input. So, how do you say actually AADHAAR is making a difference? And a brief comment on privacy of the AADHAAR number itself, I read a paper which went into the serialization aspect of it, like how the 12 digit number gets generated. And unlike say credit cards, there was not any consideration that went into protecting that AADHAAR number itself. Wherein like in credit cards you have a six digit bit code and the last four digits which only gets stored into the systems and you can even trace it back. While the intermediary who stores doesn't know what the number is. No such system is workable for AADHAAR because by design it was not chosen and what was actually considered as a factor while designing the number is that you should memorize your AADHAAR number.

Q: Yeah. NPCI is basically the big clearing house for Indian payments across and also is come up with Rupay and UPI. So, I just want to understand its relationship with RBI and what mandate it has to do all of this?

H: So, the 45% is from the Shanta Kumar Committee Report which is a government document. I think it's 2014 numbers but still relevant I'm sure. The cost of transactions in terms of moving to biometrics, so, from what I understand is that leakages have

happened between the corporation and the retailers. So, the FPA shop is the biggest criminal in all of this and any reform that has happened has also received a huge amount of backlash from FPA shop owners. So, for instance I'll give you an example in Bangalore, they've allowed inter operability that means that you can go wherever to pick your ration shop. And all these FPA shop owners in one locality have gotten together to say, if it's not your customer you don't give them grains because they're afraid of their businesses. In fact we did some back of the envelope calculations that before any kind of biometric authentication or any kind of new system which is the old one where you go and you get your stuff. The FPA shop owner was making approximately Rs. 50000 to 60000 siphoning off grains into the black markets, selling them at higher prices and all of that. But now because of these systems, the profit margin has come down to about Rs. 2000 to 3000 which is now making them unviable.

So, to me, the leakage has happened at the retailer and they are the ones pushing out the greens. And any kind of system where their inventory is calculated, where biometric authentication is required to generate, even now, they are taking 5-7 kilo off every person, I'm certain of it. But it's less than before to me. Tamil Nadu is a great example to think about when it comes to PDS because they've got several things. They've got GPS trackers on their trucks. So, when it moves from the corporation and is carrying all this grain, you know exactly where it's gone. It also has some sort of technology by which you can actually see how much the weight is in the truck. So, it must be weighing as much as it's carry or some such thing. There are Bluetooth enabled bar code readers in every FPA shop. Each bag is bar coded. So, you scan what is yours, you get a receipt from it. The GPS enabled truck guy signs it off and then finally there is a biometric authentication at the shop which means that you authenticate, it generates the receipt. The weighing scales are also connected which means that only when you get that amount will it generate that receipt.

Now, what happens once it's been transacted? That is between the ration shop and the customer and from what I understand, Bangalore which also tried to do this is that it didn't work because the ration shop guy will still be taking money off, putting his foot on the scale to increase the weight etcetera. So, those things exist but Tamil Nadu has been – and they've also increased the commissions for the FPA shop owners. So, Tamil Nadu pays some of the highest commissions in the country and that makes it easier for them to sustain their business.

G: Okay, first issue about NPCI. I think the idea behind the government company or a government organization is that, you create a government structure which will ensure that public interest is protected. If you look at basically the NPCI, if you go to the ministry of commercial affairs website and look up the board records of the NPCI, you will find that it is a public company which is a non government company. Even if banks have put on nominee directors, banks have the practice of nominating a director on every institution that they hold equity in, a sizable equity in. It means that this nominee director has to ensure the interest of the bank.

It is not public interest which is represented. So, therefore there is a huge difference between saying that, it is a government company which is supposed to protect public interest and for the public policy. And saying that I have actually a representative who maybe from a public bank, who sits in an organization, who is furthering the interest of the bank or somebody else. So, there is a huge difference. So, it is by no small standards a government company. So, I think this possibly also explains what you are asking.

So, the second part about AADHAAR and biometrics, so, if biometrics actually worked you did not need to be assigned any number. Because you could have gone and simply given your biometric and your data would have been accessible for whoever needed to access it. The fact that you are given a number, the number is the primary key which is used to query the database. And all that is being done is that, if they use the biometric which in many cases they don't, is to simply see if that number, record which is retrieved has the same biometric as the biometric which is scanned. In many cases, even for genuine AADHAAR holders, it fails. I don't know how many of you are readers of Money Life, recently Vinita Deshmukh, one of the leading journalist from Maharashtra, wrote an article about her husband's biometric failed. And he was told to go and get his biometric updated with the UIDAI. What a frustrating experience it was for them. So, it's not – I mean biometric fails for a genuine user as much as it can fail for somebody who is a fake user and as much as it can – your biometric can be copied by somebody else and misused. So, biometric doesn't automatically give the AADHAAR any status which is better to say that it's better or that therefore the records are authenticated. In fact the databases I mentioned have never been audited and never been actually verified by anybody.

So, how much of this database actually represents real individuals and ghost individuals is anybody's guess. And if you were to go by Nandan Nilekani's own figures about the telecom industry as for every 20 SIM cards there is one real user and this is in his official India Stack presentation.

Q: How are you relating both of them?

G: So, if you relate them basically if you look at the way in which the entire proposition is going today or actually for the last few years, it's about the JAM number. The Jan Dhan account, bank account, the AADHAAR number and the mobile number. So, if you really look at the way in which the financial inclusion is being pushes and actually the entire banking industry is being destroyed, not disrupted, disruption is about serving the un-served and the underserved. This is not about going to those who are not being served or who are underserved. This is about replacing an existing NEFT with an AADHAAR based payment system. It is by replacing existing KYC with an AADHAAR KYC. It is about destroying what already has been in existence in order to make a new set of entrepreneurs in the Fintech to be successful and maybe do a number of other things.

So, therefore if you look at the Jan Dhan, AADHAAR and mobile number, if you see that for if every 20 – he actually talks about, says that, you know, you have these mobile phones which now are dual SIM so, it's very easy for you to actually have multiple users use the same one and in any case 20 SIMs don't cost anything now. They are free. They are lifetime free. So, for every 20 SIM cards, there is one real user. So, if you go by that kind of number possibly even for every 20 AADHAAR numbers there is only one real resident. And you can see, linking up all of the three you're going to be able to automate a whole lot of financial transactions between different accounts without needing to be physically present and from a remote location and with no traceability. Yeah?

A: We'll break for lunch.

Session 5: Big Data and Mass Surveillance

I: Hi everybody. My name is I. First of all I'm really sorry I couldn't be here in the morning I had told S when he invited me that I was not able to be here in the morning and he said come anyways which was really nice because I think from what I heard a little bit earlier you've been having really interesting conversations. What I want to focus on is the link between surveillance and big data really which I think that we haven't spoken enough so far about in India. And there's a few points I wanted to make. The first one is that, we focus a lot on the harms of surveillance in terms of directly violating privacy rights as such and that means that there is some conception of having a private space which the state should stay out of at least in most circumstances, maybe an exceptional circumstance that can actually enter there. I actually think though there is another angle or another harm of surveillance that we need to start talking about much more and that is surveillance aimed at shaping behavior going forward. So that's not so much about what you have done in the past or what you are doing right now but actually trying to mold what you are going to do in the future.

If you look at the offline situation there's actually a lot of examples already of how that happens and we've been looking for example at gendered angles of surveillance. Looking at how in India surveillance has been gendered offline and how that continues online. And one of the things we've been looking at are the mobile phone bans that have been formulated by ‘gaon panchayats’ in different parts of India. And it's really interesting on the ground it seems those bans have actually not been particularly successful but what's interesting about it is, is that the entire discourse board about why the ban was imposed and why it didn't work in the end is about

surveillance or the breakdown of surveillance. So, the reason why a ban was imposed in the first place was because mobile phones allow young girls, unmarried women a space of privacy which they didn't have before. And clearly there were enough young women who would use that space of privacy to have conversations with young men by their families often from a community that was not deemed desirable by their family. And this in the more conservative rural areas of northern India at least by certain caste groups was seen as a big threat. That's very, I mean, the people we've spoken to are very direct about this being the reason why the bans were formulated.

In the longer term though it's clear there is a realization that technology is important in life and you can't stop people from using it but interestingly again, one of the main arguments that comes up again and again about why mobile phone should be allowed for those girls anyways is because, it provides supposedly safety for girls when they are out of the family. The safety angle though very clearly also has a surveillance angle because a lot about that is actually being able to track girls on the way to school and on the way back, being able to call them and see where they are. So, it was really around surveillance that this, both the ban and mobile phone use were framed and trying to control young women's behavior and the breakdown of control or the disruption of traditional ways of controlling behavior that happened on account of a technology. I'm telling this story at some length because I think it's really important for us to see and also I think to include in our advocacy around these issues. The fact that surveillance has control is actually a central to any system of inequality be it in India or anywhere else in the world. That is about shaping behavior and shaping behavior requires being able to control people. It's not just at the social cultural level right? It extends to governance. We see that also in the use of CCTV for example which is kind of seen as the solution to almost every safety security problem in India. So that was basically my first big point that surveillance is also about shaping behavior going forward.

Secondly I think, one of the big reasons we haven't really looked at that so much so far is because the focus has been very much on national security and of course I'm quite sure that national security arguments for surveillance will continue. But I think it's really important to look at the control angle as well because this is where the link to big data comes in. And so my second point is that, it's actually through big data and the use of big data, the promotion of big data in the surface of development that

surveillance is increasingly normalize in ways that are more and more difficult to challenge for people. When you see benefits of surveillance but then under the guise of the big data in your everyday life or you're sold practices as being beneficial to you or others in the country under that name in everyday life it becomes increasingly difficult to question the usefulness of this. It's both corporate and the government who play a role in this. If you look for example at the Facebook algorithms, a few months ago there was an update that Facebook had decided to once again change its algorithms because people weren't posting enough personal updates anymore. And for a company like Facebook that's a problem right because they need you to do that to be able to serve you advertisements effectively. If you are just reading news and talking about politics all the time that doesn't help their business model enough.

So, the change of the algorithm is intended to shape your behavior and to get you to post a different kind of update. It's not just governments that do that though and I think we've seen that there are examples of what is called database surveillance around the world. I think some of you might have discussed in the morning might actually be examples of those as well but to give an example from the West which is a long standing one is how databases were introduced in hospitals to track equipment. And so equipment was given a tracker so that you could locate it at any point in time where something was in the hospital. And the entire idea behind this was that if we are able to track where things go from department to department we'll be much more efficient in our delivery and it will be – we will also need to have less equipment because we will use it in a more efficient way. The thing is that hospitals have emergency situations on an almost daily basis and so earlier, nurses were given a certain level of discretion to deal themselves with where a particular piece of equipment was at what point on time depending on how they saw the situation in their department evolving. Those databases completely eliminated that space for discretion on behalf of the nurses. And at the same time because of that and because they couldn't plan their work anymore the way they saw it fit, increases the time that they would need to run around to go and find that equipment in that emergency moment when they needed it and then they were needed to do a million other things as well. So, it disrupted the system of organizing, it made – increased work burdens, made things actually more complicated. But again it shows like, you'd track in this case supposedly the equipment not a person and still the effect on individuals was

massive. It's also really interesting in how all the research on this issue says that hospitals implement tracking for things that relate to nurses but not to doctors.

That kind of technological imagination of governance is something though that I think we all know is very strong in India as well and especially with the current government though of course even the previous government implemented some of these programs. But his idea that you can change everything with technology and you can improve things by gathering data and making them more effective is very strong and that is of course one example. I think the push for smart cities is another one. This idea that as long as we just collect data and make people go where we want them to go at the time we want them to go etcetera, then life for everybody will be much better. Interestingly though recently there was also news that [Inaudible 9:39] Former Planning Commission now has a notch unit. And so the idea behind the notch unit is again to gather information, to be able to make both advertisement and implementation of all kinds of flagship programs of the government more effective by slowly nudging people's behavior in the right direction drawing on behavioral economics and psychology. Now it's hard to criticize these kinds of initiatives though and especially I think in India or in the developing world where you can clearly see that there are massive needs. These programs are sold in the name of public good. Who are we then to stand in the way and say like, okay maybe one can criticize how it works exactly but can we question whether they should be there or not at all? This is really hard. They can be used for the better in society. Where I think though the big problems start to come in is that we never know how these data sets are being used, what is being collected exactly where, what they hold for you. And I do think it's important to start putting these questions on the table much more because they also really relate to who has power in society. If data can shape behavior then it's important to know who has that data, who can make those decisions, what kind of data they have. And to let it just go into a black box that some people control and most of us don't, is actually really, really important issue.

I think in the long term this is a question really of democracy human rights in general and very much linked to any struggle for social justice. Going forward if we do not start to ask more questions about how this new infrastructure is going to be implemented it will – struggles for equality, human dignity will run into a new set of barriers because of new inequalities and power relations or new ways of strengthening existing

inequalities and power relations that are created through these big data exercises, databases etcetera. And then finally so, going forward, there are two things I think we need to push forward. One is to collectively be far more ambitious and I think you already heard some examples from Europe in the morning and I think J will also speak about some ways in which this is being addressed in other countries. But one interesting thing was I went to Germany in September and just a difference in terms of, in a hotel in India, the amount of data that is collected every time you check in is quite massive actually. They keep copies of your passport, you have phone numbers, email IDs etcetera. In Germany hotels are not allowed to take a photocopy of your ID. They can ask you for your phone number and your email ID but you can refuse it, so, it is a consent based sharing of information. And I thought that was so interesting because in India we take it for granted that this is something that you just have to do right? And I would think that Germany is not any less concerned about national security than India is. So why is it that this is possible in one country and not in another?

I think it's really valuable to start looking for many more examples not to say that we need to necessarily do exactly the same thing but to think about what is possible and think more about, so, where do we want to draw the line in our society? So, even in terms of big data I do think even in when it comes to using big data for all kinds of innovation and development, in Germany the restrictions are such that companies do feel tied by it to some extent and they wish there was somewhat more leniency than there is at the moment. Perhaps we can't have as strict a system as they do perhaps we don't want to but perhaps putting questions about transparency of data and who holds it on the table much more is something that one should look at. And the second point going forward I think is that we need, the whole struggle for privacy which I guess L will talk about more or the next session has really been complicated by the fact that for many people it remains such an abstract concept. And I think that's partly because so much of our advocacy has been in terms of that national security discourse. And fighting against that to some extent is complicated because, I mean anybody who lives in a big city, in Delhi has had bomb blasts happening close to their house at some point in time and then having, when this comes so close to home having discussions about this with people is just much more difficult. I think it's really by looking at how surveillance shapes behavior and drawing parallels with things that we've already know are happening and that are relevant to people in their everyday

lives like that gendered surveillance that happens to mobile phones etcetera that we can create a much wider movement for privacy protections in India than we currently have. That's what I wanted to share, thanks.

J: Is it questions first or do I go?

A: You go.

J: Okay, cool. So, apologies if I speak too fast I told me to eat some 'gulab jamum' so I'm just running off of sugar and syrup that's in my system. Just kind of hold up your hand and tell me to slow down I'll be happy to help out. Yeah, I guess so not to duplicate the fantastic work that I did, I've set about this presentation in trying to find some examples of where people have cantered that normalization of surveillance. And we could maybe go and discuss the more about what we see as being useful about them, where there's a disconnect between the example in the Indian experience. And I think generally it's just a good thing to look at because being a privacy advocate surprise, surprise I agree with the idea that the normalization of surveillance is a problem. So, we can all be on the same page there. However, there are success stories out there and the important thing is that we learn from them and we adapt them and turn them into our own success stories in our own work. So, I'm just going to focus on to and we'll see where it gets to in terms of open discussion.

So, our first one is from a Latin American organization called Tedick. Tedick are like seven people working in Paraguay, very small group but very cool. And they were, they came across a data retention discourse in their country and data retention is a policy that requires service providers to retain some information about or all information about their subscribers. India has it in, it's in the IT Act 2000 I believe. The discourse in Paraguay was around criminal investigation much like a lot of the data retention discussion that have taken. Mathew: place around the world. The bill would require communication service providers to store meta data of all internet communications for one year and it would be accessible by Paraguay authorities for criminal investigation purposes. So, Tedick had one aim they wanted to oppose the bill. They wanted the bill to be off the table and they didn't want it to be happening. They wanted to do that by using wide reach and public support. So, the task at hand for them was to create a narrative that the public can identify with, that would create momentum to hold the bill. Pretty simple, I think we've all had those kinds of

meetings right? We'll go, that's all we have to do and we've solved it. And then all the options get on the table about how you begin to do that. So, let's run through a few options that Tedick could have gone with. So, they could have gone for the principles of law argument. They could have pull down the Paraguayan constitution, began to talk about rule of law, thrown around the principles of legitimacy, necessity proportionality and really spend a lot of time just discussing this kind of principled argument. But the question remains, does that meet the task at hand? Will that really resonate with the public to let them move behind that bill? It may work in an intellectual level when you meet with different policy makers but are those policy makers going to meet with you unless you're able to articulate that the public supports some position that you're trying to make. So that's one consideration. If people want to jump in and go, I thought about this and it's a terrible idea we should never try and talk about principles of law with the public. Like, please do I'm more than happy to hear that.

Another option could have been international norms. Data retention is a very interesting discourse and in 2014 it was undergoing a lot of, it was undergoing a lot of scrutiny. So, in early 2014 there was a court to justice the European Union judgment that struck down the data retention directive that was in place across all 28 member states. It made it actually void initial which meant it essentially was treated as though it never existed. Ridiculously a huge resounding judgment premised around the fact that this was suspicion list mass surveillance that you cannot just have all subscribers have their information retain for no other reason than they are a subscriber and that they use more communications and that sometimes bad things happen as a result of that. It's a really, really powerful judgment. And there was also a similar judgment in Asher versus Brazil in the Inter American Court of Human Rights that placed digital data or meta data on the same level of protection as personal data. So, they could have gone with that. Played on the Paraguay's international perceptions and the kind of ideas around what kind of country are we creating in Paraguay, how we will be looked at around the world with all this negative data retention feedback.

Finally they could've gone for a technological assessment. They could have researched and describe the technical system for retention, lay out how it operates, who may be supplying system, identify the technical security systems that risk that data and then run that with the public. Try and generate this concern around the

database state and that if you create a database it’s not just for the Paraguayan authorities but any non state act that might be interested in it or like a hacker or another government. They went with none of those at all. They set them all aside. That was not to their mind what was going to win. What they did instead was called Pyrawebs. So, Pyrawebs requires a little bit of Paraguayan history to be schooled to you guys. Paraguay had a military dictatorship from 1954 to 1989, one of the longest running dictatorships that had ever taken place. So, going on for 35 years a lot of the people that were coming of age at this time were beginning to become politically engaged were remembering what it was like for their parents to be in this military dictatorship. Pyragüé, was a term that was used from that era, about informants of the state. They’ve described it to me as meaning, hairy feet, I still don't know why and why that matters. But it doesn't…

Q: Hobbits?

J: Huh?

Q: Hobbits.

J: Hobbits yeah, distrustful hobbits exactly. But the point is that it doesn’t have to resonate with me. The task wasn't to resonate internationally. It was to resonate with the Paraguayan people. And by using Pyragüé and turning it into Pyrawebs what they did was create a moment in which people were able to innately understand the problem that they were trying to create. Essentially it’s an oversight argument. It’s nothing more fancy than what kind of system are we creating and look at our fragile democracy that is just still, kind of, coming out of this dictatorship, are we sure that we want to begin to create the systems that could so easily fall back into control? Probably a debate that's now taking place across all pay desks in the US and discussing why did we expand our intelligence agency capabilities so much? But it's a simple thing like that it was a very simple, quite emotive but ultimately it's an oversight argument packaged up in a bit of historical realism as well. And they did the same things as any good campaigners would do. They got on the media, they used all the cultural references they could, they use Twitter to a great extent creating this thing called, I vote for the people, note to Pyrawebs that use the kind of guerrilla graffiti thing to create a more a more kind of and punky attitude to the situation. And they did analysis and they were having, they were running events and discussing this on an

international scale with groups like Amnesty International but they were always driving this forward under this banner of Pyrawebs. That picture on the top left hand corner is them handing sheets of signatures of a petition to congressman saying, this is how many people are concerned about this situation, this is how many people are not willing to accept this. And timing was everything in this.

So, on the day of the bill being placed in front of the chamber of deputies, it wasn't the data retention bill that was on the front page it was Pyrawebs that was on the front page. What they'd done is they'd taken an additive over. They weren't talking about data retention bill anymore they were talking about their own campaign and other people were talking about their own campaign. And Pyrawebs was trending as the second top on Twitter at the time as well. And ultimately those seven people that are standing there from creating a small communication campaign had manufactured a situation in which the bill was rejected firstly out of hand by the chamber of deputies at the first steps of the parliament. And then subsequently in June 2015 it was rejected in a vote in the Senate. This group of people had embarked on a small panicked strategy to try and disrupt this bill that seemed like it was inevitable and by using it in a very interesting and intuitive way to try and speak to people they'd countered that normalization. They'd used something that was seemingly redundant in the past to play and to say, look, we need to think about this from the perspective of what we've seen. Are we willing to create this? It's incredibly powerful. And they're great people as well very good drinkers.

So, the other one I want to speak too is probably one that resonates quite high, heavily with Indian population right now, was the, no to ID campaign in the UK. Essentially there's an aside that you can make around IDs, ID card in the discussion in Britain. It's essentially we'd consider the death nail for any UK government. Before the government, that Tony Blair proposed it, John Major the previous prime minister proposed and Tony Blair, he was the leader of the opposition at the time, stood up and said, we will never allow such a thing to take place in our constitution. We are standing up for civil liberties, no state, no government will ever create this ID card. So quickly times change and we'll see that again in this. So, the government of Tony Blair proposed cards, ID cards to be used to obtain social security services in combat identity fraud. And that kind of was hive that was the narrative under which this discussion was introduced. In 2001, immediately after 9/11 David Blunkett the home

secretary used ID cards as a way to talk about how you disrupt terrorism. But extensively when the actual bill was introduced we were talking about social services, we were talking about identity frauds less than the national security front. And it was actually introduced in 2004 and the important thing to realize is, this fight was going to last six years and no one thought it was going to last six years. But it did and it took a long time and it took people being constantly vigilant about the situation to oppose it.

So, let's do another little aim and task situation. Again, what did the, no to ID campaign involve and this included privacy international open rights group other UK groups. They wanted the bill voted down or scrapped by the government. Their task was that they had to counter the narrative that the ID card will solve the policy goals that it set to. Identity fraud, cheaper services sometimes disrupting terrorism when they feel like it and they feel spicy and they want to get up in the morning and run it that way. The problem with the difference I would see between Tedick and the ID card situation and sometimes the one that we might be presented with as well is that, if you don't have a specific policy goal but instead you have this kind of this benefit that is said to exist across all aspects of society it's not as simple to counter just that one narrative. You almost have to play the field and knowing that this thing that is going to go from identity fraud all the way to terrorism and to stopping off at social services is not going to be beaten by one message. It’s going to have to be fought with a variety of different ones. So, their options were again trying to think of something maybe something more esoteric, the shifting nature of identity the loss of autonomy and the constant need to prove you are who you say you are. And that's an interesting one. And I think I wrote that now and I thought why didn't they completely lead with that? But I think we have to remember when things are, you know, this is over 10 years ago things are different. I think the discussion of the loss of autonomy and the need to, that your identity is only legitimate once you’re able to show it and prove it some to some third party is only more of a kind of recent thing that kind of gets stuck in people's through. At the time it didn't really resonate in the same way. They could do the principle discussion, the ends don't justify the means, that would be a very messy situation, we’ll have to work in a lot of different principles.

Or they can look at the private sector as well. You had IBM and Thallus contracting with the government for this, play on this whole, what will they know, who could they

share the information with, the cost of the information the systems as well. They had to go with all of the above because like I said this was working on so many different factors, because this was playing on so many different policy ends. They couldn't just focus on one. They had to focus on every single one that came up. They to engage in a consultation, they had to develop the paper, they had to figure out why this wasn't going to work and then they had to feed it back in. And that's a tough ask. And it also relied on, the campaign also relied on a strong second types in the UK. So, six, I think it was four or five times sorry, the House of Lords rejected and went against the government if you continue to propose the bill the Blair government throughout their both parliaments because it ended in 2004 and then they got reelected in 2005. The House of Lords kept on saying, we're not okay with this, we're not okay with this. And they were, the House of Lords were emboldened by having these groups continually feeding them information and continually working to counter the narrative that was taking place. But it was becoming more and more difficult. And in fact the bill eventually was passed and the ID card system was being rolled out.

But just as I say the ID cards discussion always signals the death nail of a government. By 2010, a new government had come in. And the political winds had changed. And in fact the ID cards, the ID cards act is what I should have said, not a bill, it was the first bill to be, the first legislation to be scrapped by the new Conservative Liberal Democrat government. And who was the one standing up and saying, this bill is the first step of many that this government is taking to reduce the control of the state over decent law abiding people and hand power back to them? But our future prime minister Theresa May who would now never be caught dead saying anything like that. And additionally we had, private international had done a lot of work in trying to explain how these bills and the proposal would dis-empower minorities whether that be through, whether that's ethnic minorities or cultural minorities. And the Trade Union Congress, their response to this discussion was very much in line with the disproportionate effect that it would have on black and ethnic minority citizens as well. The campaign was not won perfectly and succinctly because of the argument. It was won by a whole bunch of different factors. Sometimes you have this speed of influence that you can truly, truly leverage. Tedick showed that they were able to get the public on site and they had that speed of influence in the end to truly turn it around. The ID card situation didn't get to that stage. But they did have enough of an influence in some of those rooms that once it got out of their speed of control and that

something like a new government was enough to turn this around. And the new government relied on the arguments that were being presented day in day out by those groups. Sometimes you just have to rely on the beneficent of democracy which sometimes, at this stage doesn't feel very beneficent. It doesn't seem so informed but sometimes it can be.

I think the other thing we have to realize and I understand that situations are different when we look at how groups can operate in India. There are obviously restrictions in a way that people can advocate depending on the kind of funding and the operating circumstances. And I am not saying that we all need to become essentially communication apps, communication experts knowing how to win the, or knowing how to win the public over by using scare mongering arguments. But it's about, if we look at both of those examples that was about figuring out the task that they wanted or the aim that they were trying to do. And once they've figured that out, once they'd lock down the task that was at hand they didn't waver from there. They didn't create a new task halfway through the principle, the discussion. They stuck to their guns and eventually those things paid off. I think that's what's truly important here is that, it can be a very tough thing particularly around – I mean this doesn't even go into the notion of higher corporations are having this effect on us. But if we are steadfast in our determination that this is the way that we want to create a different narrative and that we are convinced that this is the way that we can go forward, we don't waver from that. We continue to keep on pushing that but because it takes a long time for messages to sell in. And so I think, I just hope that it's more of an experience to see that there is opportunities out there, there are success stories. And I am interested now to hear about the narratives that are being used to counter this normalization surveillance in India and maybe why it's not working. In the Tedick example which I still think is the one that I'm most impressed with just because of how little chance they had and how well they did it.

Think about the unique aspect of the Indian experience. What is it about the Indian experience that will resonate quicker with the public than having to explain a whole bunch of other precepts? Whether that be technical standards or rule of law standards but something that everybody can feel in India. Something like whawas getting towards by talking about aspects of inequality or the social aspects of this kind of

thing. Is this a quicker way to get to your point? But I'm more excited to turn it over and listen to you guys. So, thank you for listening to me.

Q: Thank you. I think those were two very interesting presentations that also speak to each other in so many ways. And I think some of these are also going to time with next panel as well. I was trying to, while listening to I's presentation I was trying tease out a little more the idea of surveillance influencing behavior, right? And thinking if we've looked back or studied the ways that – for example, CCTVs in public spaces has changed our behavior or our perception of what public spaces are or how they feel to us for example. And also the way in which mass surveillance is being explained and normalized through a process of either passing it off as national security or counteracting it with convenience. So, when you have metro, you have the metro recording surveillance and seeing electronic footage is being recorded on this train but then it's also countered by the message of you are safe on the metro because we have cameras, right? Or you have the chairperson of Reliance Jio saying in an interview that, the strength of our business lies in the fact that we have data from all users and we'll be able to analyze it. But you have that being countered by the fact that they giving you free and virtually free data and so on and so forth, right? So, there are, there are multiple ways. So, one way is the national security thing but there are also economic and commercial ways in which surveillance is being normalized as we become a part of these systems. And I don't know, I'm just putting these out as things that we can think about.

Q: My question is actually to both of you I think you made a very important point about surveillance by these cameras all over the place, all over the country, in every apartment block, everywhere you have cameras. And I think most people don't pause to think that many of these cameras actually which are IP based are transmitting data to their home location which is outside your control. And unless, you know, you really know how to disable that you probably can't. So, in the name of security you might actually be enabling people who want to commit a crime to actually, or intervene a national security to actually see what is happening at a location which is supposed to be made safe with the camera. And I think most people are unaware I don't think even our defense establishment is aware about, you know, the fact that their very safe cameras in defense establishments can be seen by people in China for example. So, I think that leads me to the second question about, you know, what Mathew pointed

out in terms of, how do you run a campaign and how do you actually make people aware? So, I think while on the one hand I think there are no laws which allow any agency in India to put up surveillance cameras. It's impossible to fight a battle and point out to the police or the municipal authorities or to state governments or central government that, look, you are not empowered to put up a camera there. On the other hand, I think a campaign which relates to saying that you actually made my place more insecure. And also the fact that if there is an additional camera put by somebody else I don't know whether anybody would notice. Or if a camera is replaced I don't know if anybody would notice. So maybe you want to respond.

C: The question that I mean you were asking what's happening here. I think some of the things that made it difficult for us to fight this better here one is that there was a general sense that government is inefficient. Yeah, yeah, they'll keep asking for us nothing will happen anyway. So that lasted for a good bit. Then I think the second thing was that there was a huge corruption discourse going on. And it was in all kinds of ways and it was in all kinds of unreal and utopian ways but anything done in the name of corruption therefore they said, let's give it a chance, let's try it. So, it became difficult in that sense. The third thing is that this is a project that had not the politicians selling it but a man who has marketed all his life. Marketing the idea. So he's a good marketing man. He should actually given multiple awards for it but terrible for public policy. So, that again was another thing to be going countered.

Fourth thing that's interesting is that, one way in which he said it that one of the either World Bank or center for whatever governance in the US, the way he said it was, he said, we knew that there would be opposition to this. So, we had to create a body of opinion that would overwrite all these people. So, he did two things one was that he got in early even before we knew about the project he had got in and he had spoken to all the chief ministers, secretaries, you know, got many MOUs in place even before we even knew about it. So, by the time we started the establishment in any case had already had their power points. And they were not looking at anything else. So, that was, it was a very clever way in which he turned them off asking for materials and for proof, for evidence of how this would work into a power point kind of mode. Where he said, this is what will be done and I am the techie guy and you know it and I'll give you whatever you want. So he's done that time again. So, these are the kinds of things that made it difficult. But what made it possible was also that the, I mean some things did

happen. It’s not like, we didn’t have the whole project scrapped but two three important things have happened. One is we’ve, there is definitely not the kind of legitimacy that he thought this project would have. It does suffer from a certain, you know, everyone even people who go by the project say that there's a trust deficit. It didn't just come from nowhere. It came because people have been working on it. All of us have done various bits in different places, used every forum whatever.

The second thing is engaging with the government and government agencies. The first time they had to come, they had to buckle under and say, all right we will produce a law, was when we coerced the Planning Commission to have a meeting. In the Planning Commission with everybody sitting there they had to make a commitment that they would be bring out a law. What has made it very difficult to do anything and then we got the court, you know, you have to catch the court at the right time. If you went too early, they would say that there is no cause at all. So, you had to figure out when it was all right to go the – and then you go to the court the court takes about nine months for it to say, oh maybe we should do something and, you know, issue a – but every order of the court, even an order which was somewhat not in our – well it was doing, it was, cheering was held so that the court could give what the government wanted even that reiterated all that we had been saying. And so, six times we've got orders from the court saying that the government can't do what it is doing. Here we do not have a rule of law society. So, the government completely breaks the, you know, it's just in contempt of the court all the time and it doesn't care. And because there are so many things pending in the court, a contempt of court case never comes up. So, they’ve got away with it. But they were forced into a position of again delegitimizing themselves when they passed the law.

So, I could go on telling you step after step how it went forward and went back and forward and back. So, it's not been a win-win lose-lose situation. It’s a complex story.

J: Yeah.

Q: This question is tied to I. So, basically the key two points that you made was about was data being gathered in the name of public good and the safety through surveillance argument. So, pre big data, you know, where you did not have technologies or technological infrastructure enabling large scale data gathering and data analysis, State was still gathering data in multiple forms in various places. I mean

in India we had NSSOs and all, the surveys that we that used to do. And there where schemes that were run to optimize a certain kind of behavior. Justification was that this again will help the delivery of public goods. So, how was it that you dismantled this argument? The State sort of says that, I will optimize behavior to efficient, to enable efficient delivery of public goods. And how do you counter such an argument? Is there's anything that goes back to how it's being done elsewhere then it will be interesting to listen it.

J: I think that's a few to begin with. Is that is that enough to begin? I think we've got a few to respond to. Do you want to take any? Okay. Well I guess in that last, I'd also like to pitch on the last one. I mean when it talks about the delivery of public goods in the use of technology in doing that, it depends on I guess it depends on where the technology is fitting in. Is the technology defining where that, where the goods will be moving toward? So, this about delivery of services and they're gathering, they are prioritizing the delivery of services based on the data that is taken from some kind of measure you'd have to ask, who is that measuring. As in, does it exclude somebody from that measure? Is there a censor out there of some rural society in India that truly would actually benefit from receiving these services before anyone else? But actually because you haven't gone and put their censor or the measure there you've just excluded them entirely from the delivery of those services. And I can guarantee that in every single circumstance where somebody's tried to develop public policy based on just one measure they will have done exactly that. Whether it's through an app that can only be installed on an iPhone which then takes out all the [Inaudible 9:19] members of the public who either have got android or even not at all. These kind of things will, are figuring more into public policy and having a negative effect. So that's one way to change on those.

In terms of the very first questions of like, how we move back against the economic incentive, the economic incentives argument in terms of like, give us your data you get free, you get good services, it's a tough one because it's very winning and very persuasive. I think one of the, I think a part of it is you've got to look at and particularly in the Indian situation I know you don't have the opportunity to hold those statements to account. Like, literally you don't have a data protection framework that has an accountability mechanism, that has an authority where they say we'll give you these services and you give us this data and you will truly benefit and we will be in a truly

equal and an equitable relationship of what you're receiving and what you're giving up. Data protection authority while isn't, while not perfectly empowered to do exactly that and weighing up those things, we'd at least give you some opportunities to begin to hold that statement to account. So, you can call BS on that a little bit and say, well look I can't hold you to account for that because we don't have a data protection framework and you continue to push on that and you continue to tell people that, well you can't say that because there's no proof, there's no way of us actually like looking at that information because there's no way of us getting that information to truly interrogate it. And that may lead to you having a data protection authority at some point if you get enough of a wind behind you.

But in the national security front it's an asymmetrical war because there's always going to be more information or information that will always be withheld from you because they have to withhold that information. You'll never truly know the effectiveness or why something needs to be done because they'll say, we have to hide it for these purposes. But on the – but again in almost every circumstance, there is always more that they can give you. In fact there is, we started with our campaigns in the UK against GCHQ, we've won consistent legal battles against them and making them reveal information that surprise has not led to the society crumbling and as a result all of our state secrets tumbling out. But we have learned more about what our intelligence agencies have been doing. So, in every circumstance when they say, we can't reveal this information or we can't give you that, they're always there's always more information they can give. And that can either be a court case or a bigger push in a more kind of intellectual framework. In terms of the more difficult one which is on the street, national security that you're getting from the CCTV, I think the doctor's example is a good one. You begin to say, well it's not just us here. It's not just the Indian government that's involved in this. The Chinese are as interested in this. Foreign state actors are as interested in this kind of information and vulnerable equipment is easily, is being used day in day out now for attacks. Whether that's DDoS attacks or even like accessing sensitive data.

There will come a day where critical infrastructure will come down as a result of the internet of things like without a doubt because we continue to have bad systems. And unfortunately we're a reactive society and I don't mean that just in for the UK or for India, I mean that like a species. Like we are reactive. We don't look, we don't see the

problems that are ahead and we only go, if only someone had told as this was going to be a problem. And then we try and fix it afterwards. That's just the nature of how we live but I think the more we continue to put those things forward and to show that there have been examples of around other places that you may be able to win at least some minds in whether that be the department of ICT or the Data Security e-Council of India or even the CSG or the [Inaudible 13:22] whatever. Like you can win those maybe you can win some of those intellectual fights there. But those are I don't even know if I'm answering all the questions but those are some, certainly some points you can take forward I think, hopefully.

I: Just on the last question, I think to some extent all of us also want to give our data to get better services. No, it's not as if we don't at all no, but that's also too. I really think it is about the frameworks in which that is embedded. In terms of like pre internet data gathering and now, one big differences that earlier a government or any player had to decide beforehand what they wanted to know and then ask you to please tell them that. It's a very focused kind of data gathering. While at the moment and especially the more databases or initiatives are being linked, the depth of data that is being gathered and what can be concluded about you just goes far, far further which is also why these issues have become so much more pressing. I think at another meeting where C and myself were yesterday you asked that question of like, why did the government go and protest that we have a fundamental right to privacy in the Supreme Court now and not 10 years ago? Because not having it now gives them additional benefits which did not have the same kind of relevance 10 years ago. And to give you a sense of like what, the kind of stuff you can gather from big data, the founder of OkCupid wrote a book called Dataclysm which is really worthwhile reading like on a flight or something. It's easy reading. Among other things what did they find looking at the data from people who wanted to date and subscribe to their service? This is, the population was American people who use that service.

As the age of women goes up the age of the men they are interested in, going by the pictures they click on goes up as well. That actually more or less matches what they say on their profile so the age range they give on their profile matches the age range of the pictures of the women they click on. This was heterosexual people only. For men, they also say that as they get older the age of interest increases. But the pictures they clicked on overwhelmingly was of women between 20 and 22 years old very

systematically. Now this is really, really interesting data from a feminist perspective which we would never ever have found if we had asked those men that question directly.

I think the gap is put on a graph also and when you see kind of like, the difference between the two graphs is so striking. He has something similar actually for racism and dating. So, sexual preferences at an individual level, people will note, the people who use OkCupid by and large are liberals in political leanings. So, they will not say that they are, that their preference would racist. But overall black women are very clearly discriminated as being non favorable partners on the website and it comes out in the – and it's specifically black women. Not Asian women, not white women, black women. So, it's, you know, these kinds of things, you wouldn't find out that kind of information. Not on that way.

C: Not in that way but these are things we know. Why do we want to go to a digital medium?

I: No, but so I'm not saying – I do still think these are the arguments that will be given, no? That, isn't this interesting? The thing is like, do you really feel that your government or a company needs to know that kind of intimate things about you? And then of course the argument will come out that you only need, like these data sets are anonymized so what's the problem? But actually credit to him, even in that book about OkCupid, the author says himself, in most studies with four data points social or spatial you're actually able to de-anonymize something like 70-75% of any dataset. You don't need to know much in a dataset to be able to see exactly who it is. So, I think those kinds of things we need to think about much more. So, what does that then mean in terms of data gathering? So, I'm not trying to make a point either in favor or against but, how many people know these things no? This argument of that, oh it's anonymous, is so widely used. There are universities who did research in like the campus, and anonymous supposedly, and stopped because they realize that they could figure out on those very sensitive issues they were looking at within no time who the students were who had responded to their survey. So, I think that's kind of the bigger point I wanted to make on that.

On the CCTV thing so as part of the work on gender surveillance we're doing we're looking at CCTV also. It's early days so I can't say much about it but what's interesting

though, what you see in the literature also that actually in actual practice, what you were saying about, it makes you much more insecure comes out also for example from a gender perspective. In India we have seen that when that video was leaked of all those couples on the metro canoodling, which is again, it's all done in the name of safety. But actually across the world you see that CCTV which is done in the names of women's safety gives men who are at a distance additional space to observe you without your consent. And while an actual incident happens because guards are replaced by CCTV there is nobody for you to draw on immediately and ask for help. So, the issue of, does it actually even in that, you know, it's not even about the national security hacking whatever. This is about very kind of here and now. It isn't so clear at all to what extent it does increase safety even if that's the discourse that's used in India. What I also think is that, the class angle of, coming to the point of what's specific here, I think there is a class angle to surveillance in India which is different from what you have in many western countries. Where traditionally in the west, like in the US it's black neighborhoods that need to be under surveillance right it's an indication of, deviance or criminality, at least pre internet that there was surveillance.

In India, we have airport like security in malls but not in lower class shopping areas. We have that in the metro but not when you take the bus. The first people who wanted to have CCTVs were expensive shops and middle and upper middle class colonies who wanted to have, who themselves wanted to have cameras at the entrance of gates. So, it's kind of a way to distinguish yourself also that we belong to a certain class, we create our own security. That is done through this constant surveillance. I think it creates an additional angle of complication and actually when C was talking about the monetization now, cashless economy. I find it really interesting how some of the discourse that comes out in the media now is about having big notes at home is almost seen as moral deviant. There is a moral judgment about this. And even say like women who have kept money, who have controlling husbands, no independent access to resources and without their husband's knowledge have tried to save money on the side that's judged negatively now. Like, haha let us come out so we can all trace it. I think again it shows like it's almost seen as if, allowing yourself to be surveilled this part of that middle class, safety, honesty, we're also upright citizens kind of a model, which actually is a really controlling way that completely ignores also the inequalities that exist, the sensitivities that are there in society.

So, yes I think that was my argument. I have a question for J as well as though. And for everybody here because what I find really hard in this debate is, the examples and this is usually what happens right. Like I think save the internet in India was an example of a really effective campaign that in many ways did things similar to what you are presenting here. But it was facilitated by the fact that there was like a very clear policy process. And it was also quite clear what were possibilities around it. I'm by no means saying that's the only reason it was successful because we often have those opportunities and don't make the most of them but still, I think that helps. One of the challenges with the normalization of surveillance I think really is that it comes in so many different forms and places. It pops up everywhere and it's again – so, in Bangalore in that hotel where we were in additional – to when I registered in addition to everything else we had to do, they also had this little CCTV camera and wanted to click a picture of everybody at the point of registration. And I actually refused and it seems I was the only one but they didn't take my picture because I was like, there is no police requirement for this. Why do want to take my picture? But it's interesting how again like this idea of, we just need to use these things more and more and do it everywhere and have it – so, how do you fight back against something like that in that circumstance, right? Because we can focus on like – even if we would be able to fight that they're doing a zillion other things right, the government is doing a zillion other things that draw on exactly the same principle. It feels like, how do you do deal with all of that at the same time? That's such an easy question for you to answer.

Q: Oh and in a country of 1.28 billion you just do this 1, 2, 3 no, no, not all. It is a incredibly difficult. I think some of it's going to organization. Like if you put, if you get together with one within your different civil society groups and you look at the problem and you say, we're all just going to take on this thing and like that's the only thing we'll fight. Of course you're going to create, you're going to let the other problems slip alongside and as a result not be able to cover all those bases. There is a level of better collaboration across civil society whether that plays on people's ability to communicate or people's ability to research or people's ability to make connections in policy fields. Knowing where their strengths lie and having them focus their efforts on that particular area rather than attempting to become a Jack of all trades in certain ways will at least provide the beginnings of an opportunity to start to work on that. So, better collaboration I think across civil society helps.

But in terms of those like very, very – I actually think like your example of the Bangalore hotel is the, it's like the little small act of like resistance to a thing that's just stupid. It begin, it's a small like trip towards it. I don't know why your example immediately had me thinking about a problem, a thing that happened in the UK was, we found out there are, one of our retailer's booths when people were leaving the airport they would scan their, they would ask to see their ticket so that they could claim back VAT. But often that benefit wasn't being passed on to the consumer and it was being retained by booths in the company itself. And that was revealed and as a result this like small little thing of like, now everyone goes, you're just going to use it to benefit yourself and no way do I want to help you get better at this. And that kind of, that sort of expose that only lasted like two days in the paper has now – it actually switched on normalization and no one gives their airport ticket to a booth member or staff anymore. They say, I don't have to and I won't because there's no requirement and we don't and we now no longer trust them. But like, that's – these strange things you never know what is going to work. You never know what's going to be the light, the touch paper that's going to turn it around and make society discuss that it's some kind of weird bit of data collection. But in the booth thing that was that we just didn't feel the benefit from it. I think you just have to try almost everything. And something as simple as, I don't need to do this. If somebody else saw you do that in the in the reception, in the lobby and they might, why do I have to – I don't want to do either. Unfortunately you were the only person to do but that lays the seed. Surely that must lay the seed in some other people, you – a small aberration in the normalization framework can lead to very, very interesting results. And I think that's the, I think you just have to practice what you preach in those kinds of situations really. And that is 1.28 billion, you know, just one at a time just keep working it through as we are talking about it.

C: I think one of the things that the project did right in the beginning was give the people with a low, you know, with a great low self esteem, great low self esteem, a sense of them being unique and flatter them into participating in the program. I mean I think there are, there is a certain way in which suddenly they felt themselves being identified. This is the middle classes this is not, most people got bullied into it. But there were people, you know, when you had asked them, so you went there and then you put your fingerprint and you gave your ID, you didn't have any problem doing it. And they were like, but they asked for it and each one of us is, you know, we are

unique, my fingerprint is unique. And like, how do you know? So, for a spell, flattery worked. And there's another thing that no amount of evidence seems to be enough. The amount of evidence that's been, that's got accumulated by now what trashed this project is, no amount has been enough. And that I think it will help us if we can unpack why. How it is that, nothing seems to make a difference?

J: I would also recommend that actually doing a why after any action like sitting down and debriefing so often we just move on to the next thing within civil society because there are so many problems we have to deal with. We don't even have a chance to review what do we think worked, what took way too long and didn't really work and we could have spent doing something else. And you begin, if you have these long debriefs that are painful because a lot of it's about how you didn't do it right, you eventually come on to tactics. And without a doubt when you hand the government a defeat they're doing that. They are figuring out how you won and then circumventing that process the next time. You got to do the same thing because it's – otherwise we just won't repeat the mistake again I think. I mean that cross like regardless of India, UK does it is well we need to do it more often.

D: So, here's a question you know. I'd like your thoughts on the typical argument that is put forward that, this is too large to fail. So, just like Wall Street is too large to fail now AADHAAR is too large to fail. So, you know, how do you counter an argument like, too large to fail?

Q: My question was just a follow up to, I don't know if it's a question, follow up to C that, you know, when you say that there is no amount of evidence is enough and you are implying there is a lot of evidence. The problem I, at least as I see it is that there is a lot of evidence yes, but a lot of it hasn't trickled down to the masses. If you want a – yeah, it's all at the intellectual level. And these days an added problem is that if you want to build up any sort of narrative and any sort of past movement you need to go via social media. And Twitter has a 140 character limit. So, if you want to explain something it's got to be very simply.

C: No, I just want to follow up on that as well. The idea of participation, of making people feel important I think that happened this time with the demonetization as well when Modi stands up and says, 'humare maha yagya mein ahuti dijiye' and suddenly everyone's telling me, oh my God I feel like I'm contributing everyone's inconvenience.

So, this has got to be something great because, look at us, we're all inconvenienced at the same time. And as much as I told everyone, you know, this is not going to work. My parlor lady in fact was telling me, 'nahi', if they're doing something this obviously means something because, you know, I am getting to participate in something that everyone in the country is doing.

Q: We all suffer together.

A: You have a quick answer to that too large to fail question?

J: Too large to fail, yeah, I so, I unfortunately – so, what happened in the UID, in our ID situation like I said, it actually came about an austere argument where they said, this is too expensive and we're not going to do it. And so it was being slowly piloted at the time. And in fact a whole bunch of people who paid for the card itself and the government said yeah, you're not getting refunds for this. So, it's about 90,000 people in the population and they scrapped it. So, that's the only experience I can pull on in terms because the AADHAAR program to my mind has gone further than any other program that I've seen. So, I've never come across a too large to fail argument necessarily in these kind of spaces because the investment has never got to a point at which, instead it's more potential investment has led it to being scrapped because austere times it required some government services to pull back on their developments. So, unfortunately I don't have an answer to that argument. You guys are – because you're quite far down the line. I don't know how to, I mean what are the numbers? How much money is being spent?

Yeah. We had to pay, the government paid Salas and IBM both I think in the tens of millions of pounds for reneging on the contract. Astonishingly they just kind of paid almost what it cost anyway. So, the whole austere argument ended up being a whole bull because they were very bad at negotiating contracts with the private sector or you can say the private sector were just much better at getting that, getting the resiliency in there. Yeah, I'm going to keep thinking about too big to fail though. I'll speak to you, I'll talk to you later about it.

Session 6: Privacy is (a) Right

S: Last session K and L. Not the last session. Last speaking session then we have a discussion session to talk it out. Yeah, we are just waiting for – anyone else wants to grab water. Some of you maybe dehydrated water is outside. We can wait for 5 minutes.

K: Hi. So, since this is a session on privacy as a right or the right to privacy, I thought I'd begin with articulating why privacy is a very difficult concept to define. Over the last century or even before that privacy itself has been a very difficult concept to articulate. There's very little coherence on what the right actually is and what it is that the law must protect. So, different conceptions or conceptualization of privacy have come up. You have the famous, the right to be let alone, which was put forth by Warren, at least credited to Warren and Brandeis as in 1890. But over the years, we've also seen arguments where privacy's been understood as, control over personal information or personhood or intimacy or secrecy or confidentiality. Now the divergent arguments would say that these shouldn't be conflated and say confidentiality or secrecy isn't privacy but then again there are academics who feel that privacy is an umbrella concept and it's better if we include all these conceptions together. In India too the Supreme Court has, in fact on the first case which recognized the right to privacy which was, Govind v. State of Madhya Pradesh, the court recognized that it's very difficult to define the scope and content of the right to privacy and they said that, we're going to be taking, it's best that we take a case by case approach to define what the right to privacy is. The Supreme Court has defined the right to privacy as a penumbral right which is that, you can't locate it in one

constitutional provision or one fundamental right but in a numbered, in the whole scheme of fundamental rights.

I am just quickly going to map out the Supreme Court's jurisprudence. I think that's important so that we understand where it is, the protection is lacking under our current jurisprudence. Other commentators have already sort of tried to categorize privacy jurisprudence, I'm going to borrow from that and divide the jurisprudence into state surveillance of privacy as an aspect of surveillance by the state, privacy as an aspect of dignity or autonomy, individual dignity or autonomy and privacy as an aspect of informational privacy. So, these are the three categories that I'm looking at. To begin with if we look at state surveillance, this was the first stand of privacy jurisprudence that was developed by the Supreme Court. The earliest cases which was in 1964 and then later on even in 1975 these focused more on the physical aspects of privacy or locational privacy. You had certain police powers which won the challenge so, the police had the right to secretly picket someone's house or pay domiciliary visits or check on the movements of a certain category of individuals and these were challenged before the Supreme Court. The 1964 case which was the first case which laid the foundation for the right to privacy Kharak Singh v. State of Punjab, it didn't expressly incorporate the right to privacy but it did lay the foundation for it. The right to life and personal liberty was understood or interpreted in a very, very broad manner and the Supreme Court also [Inaudible 3:21] with the maxim of, the common law doctrine that every man's house is his castle.

Then we had Govind which was the first case in 1975, Govind v. State of Madhya Pradesh, where privacy was expressly incorporated into our jurisprudence and the court held that the right to privacy is a fundamental right under article 21. Here, Govind is important because the court also had that there must be a compelling state interest. If freedoms or the right to privacy is supposed to be, is going to be restricted. When we looked at leader cases on state surveillance we have PUCL versus union of India in 1997 which looked at instances of telephone tapping which looked at cases of telephone tapping. The provision or the government's power to tap conversation over communication wasn't struck down but the court did sort of incorporate additional procedural safeguards that must be included. Here it's important because this case also recognized that the right to privacy was an aspect of article 19(1)(a) which is the right to freedom of speech and expression. So it's your right to free speech to have a

private conversation over a phone call. I think an important aspect to this case is that, it was argued before the Supreme Court that there should be an independent review or prior judicial scrutiny before communication can be intercepted. But this was not accepted by the Supreme Court and this remains a severe lack in our jurisprudence on surveillance. Later cases as well have maintained – we've had a fairly satisfactory jurisprudence when it comes to state surveillance privacy as an aspect of state surveillance. We had 2005 decision, the Canara Bank decision where we rejected the third party doctrine which is a part of the American jurisprudence which is that, if you voluntarily hand over your information to A party, you no longer have a reasonable expectation of privacy over that information. So, this is a part of American jurisprudence but we rejected it and saying that, no, that expectation of privacy continues to remain.

I think what is interesting when you look at the whole line of cases on state surveillance is that in most cases where the regulations were under challenge, while upholding some of these regulations the Supreme Court has always been, has always considered that the surveillance was targeted. It was never, it was not mass surveillance, you had a reasonable basis for targeting a particular class of individuals for irrational reason. This is important in the current context even though mass surveillance hasn't come up before the Supreme Court it's important to remember that, laws which allowed the state to exercise surveillance powers were upheld because they were targeted.

I'll now go on to privacy as dignity or autonomy claims. In the case of, in the context of gender rights we have seen the right to privacy be invoked fairly frequently. So, when the Supreme Court held that the two finger test for rape was unconstitutionally, it invoked the right to privacy. It also invoked the right when it held that women have a right to exercise reproductive choices they have a right to make their own reproductive choices. In a very recent case which is a 2013 case, Nalsa v. Union of India, the Supreme Court held that, self identified gender, you have a right to a self identified gender to identify your own gender and that is an aspect of the right to privacy. Again, before this 2010 was Selvi v. State of Karnataka where the court distinguished between physical privacy and mental privacy. This was a case where constitutionality of narcoanalysis test or polygraph test was challenged. And the Supreme Court struck down these tests. It held that these tests were unconstitutional.

It held that, even though you have police powers which can extract physical information say, DNA samples or fingerprints that can't extend to mental privacy and invasion of mental privacy.

High court jurisprudence on this has been, recent high court jurisprudence on this has been quite progressive. You can see the right to privacy being invoked pretty frequently in recent judgments whether it's the Bihar prohibition case which was decided by the Patna High Court recently or the beef ban judgment by the Bombay High Court. So, this is definitely an encouraging trend even though it's not like it's been a uniform trend because we saw the disastrous case of the Naz foundation case section 377 where the court refused to engage with privacy as an aspect of dignity when it comes to sexual relations, consensual sexual relations between the same gender. When we look at, coming to informational privacy, this has definitely been a weak stand of the Supreme Court's jurisprudence. Just to, at the onset, the Supreme Court hasn't considered online privacy or privacy on the internet. So, those kinds of cases haven't yet come up before the Supreme Court. We have informational privacy in very, very different context than what we are discussing today, say, big data or schemes like AADHAAR or CMS. So, you have X versus Y hospital, you have Sharda v. Dharampal, these were of course – so, just as a factual background X versus Y hospital was where a hospital disclosed someone's medical information to the person's fiancé.

So, the information that a person was HIV positive to the person's fiancé. This was challenged by the individual and the court held, the court balanced the fiancé's right to health and that person's the petitioners right to privacy and held that, you know, this disclosure was lawful. I bring this up because most data protection frameworks look at medical information as extremely sensitive personal information. Again we have a strand of cases where the court has held, if a person can be compelled to undergo a DNA test or a blood test. It's a little confusing why the constitutional right to privacy has been invoked in these cases because they're completely, you know, they are two private interests that you are trying to balance out. But the fact is that the court has. It has invoked article 21 and the right to privacy even while discussing DNA test or blood test in custody battles or paternity cases or divorce proceedings.

K: Yeah. Just a few takeaways from this is that again to reiterate that the informational privacy strand of the Supreme Court's jurisprudence is fairly weak. In the constitutional challenge to AADHAAR, now the whole gamut of privacy cases have now

been referred to a larger bench. So, the right to privacy can be – to determine whether or not we have the right, the fundamental right to privacy. This is, I think it's a good opportunity to not just clarify the jurisprudence as it stands but in the main case where the merits of the matter will be decided it's also an important opportunity for us to bring the privacy jurisprudence up to the existing threats that we see today because of the increasing commodification of data and the increasing threats from digital technology. So, there is also evidence to suggest that the Supreme Court favors targeted surveillance. In several cases, cases have been upheld only because as I said that, you know, the powers allowed the government to surveil only a particular category of individuals and not, there was no conception of mass surveillance. With respect to communication surveillance, again, lack of independent oversight remains a serious lacuna. So, that's something that needs to be addressed. Because this is even, although we have a review committee which is empowered to scrutinize these interception orders, this is completely an executive committee. There is no independent oversight or a judicial oversight over these orders. I think that's about it and then we can conclude.

L: Thanks K for lay around the constitutional background to the right to privacy in India. The right to privacy as we now know doesn't firmly exist as a constitutional right but certain cases which K did touch on, the High Court cases, the beef ban case in which it was held that possession of beef does not, cannot be a criminal offense per se. Slaughter of a cow can be a criminal offense. So, it was held that, you cannot – but merely by possessing beef you are not a criminal and there's a reverse owner's clause also there. The right to privacy was invoked there. The second case was the prohibition case. It's from the Patna High Court. Again, privacy, right to privacy has been applied both in terms of being a constitutional principle. So, it's not as if the reference is holding back the High Courts from applying it but The Delhi High Court in the WhatsApp privacy case, as it is popularly referred to, has stated quite expressly that the right to privacy is presently under consideration by a constitution bench and it's not appropriate, I think that's the precise phrase used by the court. It's not appropriate to extend it as a constitutional right or to apply it as such at this point. So, there is some degree of uncertainty but the high courts are seeming to apply to it.

Now coming back to the constitutional right to privacy, the constitutional right to privacy would be restricted in the sense as indicated by K because it would apply

principally against state subjects and would not take into account protections which are necessary to be extended against private actors. Secondly it would also have institutional limitations in which, the right would be passively enforced through court judgments as opposed to a regulatory authority which would develop codes, develop standards, enforce laws, files suits. Also a much more developed substantive framework would be available by ways of legislation. And this has been indicated by commentators in the past as well. And there seems to be a lack of movement on that. There have been certain drafts which have been leaked in the public and that's also a pattern to be noticed in privacy regulation as there is an absence of a general process of public participation in drafting and consultation. And it extends to the AADHAAR Act and the regulations made under it as well in which neither the act or the regulations were put up for public comment. Just focusing on the act right now for some moments, the act creates independent surveillance powers. The safeguards which are stated by it are arguably, and I'm stating arguably because it is to be argued. Arguably go far beyond the privacy safeguards put in place by the PUCL judgment substantively.

So, there is a, the substantive categories under which surveillance may be carried out under the PUCL judgment tie in with the provision of the constitution. And it's not present under the AADHAAR which uses the phrase, national security, as opposed to, and please remember these are terms of art being phrases of law, so, as opposed to being in the interests of a public order or security of state. So, those phrases are not mentioned, national security is mentioned. And national security is not defined within the law. Hence the substantive Traditions for application of a interception order we'll not be pursuing to legislative guidance and they will be applied by again committee of bureaucrats want open to independent scrutiny, audit provisions, oversight committee in the draft did have the leader opposition presented it, I don't think so that's innovated now it's completely internal. One point I would like to make is with regard to the technical process under AADHAAR and we had it quite a lot times in which it said that people are being made subjects, it's true to a large extent even if you look at the act and the regulations and how it's creating data if you go through the authentication regulations by itself it's making it quite clear that data is being stored by different entities and at different points, meta-data is expressly stored even though AADHAAR act by itself says in demographic data, your caste, your region, religion, sensitive topics like that will not be stored. If you have a seven year window to catalog

meta-data points all those points of information became fairly visible. Constant response to a lot of privacy arguments which are heard around big data in India is that you don't understand the technical processes behind it and they exploit a certain amount of inexperience people so they say that the technical processes will take care of it but even the technical, literature is not as forthcoming s it should be and also fundamentally technical process which has certain safeguards in place which are not found within legislation or regulation or subject to a regulatory authority post deep racists by itself. It is a front door rule of law society as we profess if not aspire to be so, as per me the act as a result regulations are problematic I'll be happy to share specific information on both points with you and assure you that even to a neutral commentator if you spend about 3 to 4 hours with them you will see problems which do arise from it.

C: Can I just quickly wrap up. So, just sort of taking off from where we off, I think a legislation is important if you – you have to have a data protection statue with – which will incorporate fair information practices. A constitutional right to privacy can only go so far, I think if we had to articulate a constitutional right to privacy because that's the subtext for this session, I think it's important that the Supreme Court recognizes the value of personal information. There is a need to exercise control over that information that and that whoever is collecting that personal information must be held accountable, if these three elements are incorporated in the constitutional right to privacy I think we have a very good foundation.

My favorite example of a constitutional right to privacy is what E pointed out what exist in Germany, which is decided in the Census case which is informational self determination which was cut out of a right to human dignity – a right to personality which again was established out of personal liberty as well as human dignity so that's what I'm hoping for.

Session 7: Open Discussion

E: I'm not so sure on this question is relevant over here, which is sectorally – it has sectorial land up by me and I wasn't very sure that I should ask this question at what point of time because it is AADHAAR actually which had taken like the major part in this. The question is for both of you since you are like – like the entire thing was to do with law. Now I'll – my question is has to do more with sectorial stuff, it's about the patient health data and the issue is with the e-pharmacy and the only simple example is in front of me is that whenever the patient health data goes onto the e-pharmacy platform the prescription is uploaded at that point of time. So, what is your take when the prescription is once uploaded and there are situations where e-pharmacy platform is where they're just intermediating they're not handling your prescription so, in this kind of situation that prescription goes haywire, it goes where? Who are – like now definitely the data subjects that is the patients if the prescription goes somewhere else say, for instance the pharmaceutical companies they make – they definitely they can make use of the data for their own nefarious purposes or whatsoever. So, now what is your take on this? Do you think that the current legislation that we have that is the SPDI IT that's simulating under the IT Act, and they say under sensitive data is that the only thing that we have at this point of time and wherein the data handler we cannot even like point out who is the data handler – what is happening after that and where the data goes, what is your take on this?

L: I think K pointed to it with the state and with the reference to Govind v. State of MP and when you reject the third party doctrine you recognize that the person by itself

keeps possessing privacy irrespective of whether the document is handed to a third party right so, the person will always have control over that data in a sense at least that's what has to be doctrinally respected. Now of course there is a absence of substantive law, there is a absence of process to enforce it and this is where we are.

E: Still I think it's sort of suspension because what – what I understood is that once you – you are holding the patient responsible for everything the data that has gone out, the prescription whatever his medical history is there which is definitely sensitive in nature…

L: There is a provision under law but I don't think so it can be fully utilized. The section 43A of the Information Technology Act and Section 72. The police department will register a FIR if you and a lawyer will help you write it in a way that Indian Penal Court can also be invoked in certain instances. The objective is to maintain security of your data a system right. So, that's why I'm saying there is a deficiency of law, there are certain laws which are covering parts of it but they're not doing it efficiently to the policy objective which is necessary.

E: I am a lawyer myself so I do understand that but I was just like you know, imagining it for the greater good like taking queue from there whether there is a…

L: Think about individual good first and let's go to the greater good after that for the individual by itself what will be better is that their records are safe and they have control over that. There is absence of substantive law – yeah – there is a absence of substantive law and absence of process and I'll keep going back to it and we need something which is specific and which is tailored to this, pending Penal Court or the IT Act with one criminal provision which is bail able doesn't shouldn't matter actually. 43A is completely defunct both in terms of its substantive teeth as well as the process to enforce it and for people who may not know how is 43 applied, it is applied through a complaint for civil penalties, damages to adjudicating officer because you cannot approach the civil courts, the jurisdiction of the civil courts is barred so, you do not go to a court and file a civil case and you may think that's a very good thing because civil courts take so much time to determine cases, you may die tomorrow your children maybe fighting that case for compensation but this is way worse okay because the case is being determined by a State IT secretary in most States and in some States there is no adjudicating officer itself who's being mortified under the IT Act because

the State government needs to mortify the adjudicatory authority which is the State IT secretary, the State IT secretaries are not trained in law, they do not have a secretariat, they do not have docketing processes, they do not know how to write the order. Now what will happen when the up – it goes in appeal, it will be set aside because the quality of the order will be so bad but the process of appeal as specified under the Act is deformed right now because the central government for the past 3 years has failed to appoint a Chair person in the Appellate Tribunal so where do you go now, yes this is Kafkaesque so you go to the High Court okay and a lot of petitioners did approach the Delhi high court. They were usually large banks okay against who awards have been given, two customers because large amounts from their account was siphoned off due to improper data management practices. The high court heard a bunch of 20 cases by itself, asked the bank to deposit the money, some people who in financial need after creating security essentially by giving registrations of their cars or giving personal guarantees things like that withdrew the money but the high court after pushing the central government for more than one and a half year gave up, help up its hands and said that all these cases will be heard by the Cyber Appellate Tribunal, now they show them the docket of the Cyber Appellate Tribunal but no hearing takes place there, you know why? There is no Chair Person there. So, this is the process we have in India right now.

Q: Hello. Hi. So, I was listening to a podcast a couple of days ago and they were talking about how with the advent of internet of things, privacy policies are not going to make a lot of sense. This whole consent based privacy is going to stop making as much sense because your coffee machine is not going to spit out an entire privacy policy that you're going to go yes or no. So, I was wondering if at the stage of the debate we are in, should we be entering that discussion of looking at other ways of approaching privacy like harms based approach or – do you think we are at that stage? Since we don't, since we still don't constitutionally recognize the right. Can we redirect the argument somewhere else instead of the practices recognized before?

L: Problem which arises is that the right to privacy is a fundamental right. Fundamental rights means it's a limitation on the power of the state. The state does not willingly enter into conversations around the subjects seeding its power, making it a conversation. That's why we need fundamental rights. So, that's why it's very important for the fundamental right to be firmly established in the broadest contour

as possible irrespective of where we enter a debate with respect to the internet of things. So, privacy would apply to a whole host of circumstances. K told possession of beef, consumption of alcohol, it's very wide, sexual identity, it's very wide. So, we need it irrespective.

Q: No, I agree there has to be a constitutional right to privacy. I'm just saying like, if you need a data protection law in place, for those practices that we want to get in, should we be looking at things other than consent based privacy? Thank you.

L: So, there is a catch up between this law and tech race. So, the tech blames that law doesn't catch up. What can law do or lawyers do around that because I see, like, developer documentation having metadata fields that explicitly say that, you should not be using this field for anything else. It actually indicates the developer that you can use this field for cookies. It's going to go, take a long time before the law comes in and then says that – because there is no penal action specified in the developer documents because it's just a developer documentation right.

Q: Actually my question is not only for L but actually like his thoughts on it as well and it was triggered by something K said which was that, perhaps the constitutional or the constitutional bench now discussing whether we have a fundamental right to privacy is a good time to get them up to scratch on informational related privacy as well and get much higher standards there. But there's a reason why they haven't been particularly interested in that earlier also I think. So, I'm just wondering like, how do you think then we should approach that push to bring that really on the table in that entire discussion and use that as an argument to actually get strong protections there as well. Are there particular cases or sectoral concerns that we should use in trying to do that that you think the court might be more open to than others?

K: It's not that there is a difference we need to make between privacy invasions of certain kinds and certain kinds of systems which are being put in place so that privacy will be destroyed. It might be easier to approach it through systems where privacy is deliberately being destroyed. Like the UID is one example but there are others too. So, that's one distinction even within the idea of privacy itself. And the second thing that actually the argument that was made in the court on this was a very effective argument except that the court was too lazy to pick it up. The basic thing is that till 1969 the way the constitution was interpreted, it was that the state had certain

powers and you had to, an individual, you had to explain why the state did not have the power to treat your rights in a certain way. And you had to be able to say specifically within which fundamental right or fundamental freedom you were laying your claim. You couldn't say, my right to privacy is both in article 191A which is freedom of speech and expression and article 21. They said, tell us precisely where it is because the state, you know, if you're attacking, challenging the state, then you need to be able to say precisely where it is.

1969 that changed and that was by a large bench which said that, the way you interpret the constitution is through the rights of the people and not the power of the state basically. So, that had changed by then. This was a completely spurious argument that was made in the court and the court just walked into it saying, okay, you know, we agree that there would be no constitution and no fundamental right at all to life and person and liberty if you did not have the right to privacy. But in the interest of judiciary disciple, which discipline is lacking in so many other things, they decided that they would have to refer it to a larger bench. So, it's a completely facile and stupid argument. So, if they do anything with this it will be because they don't want to give us the fundamental right to privacy not because it is not recognized in the constitution. And one last thing is this that, you know, the 1990s when the economy opened up and they felt they had to give everything to everybody, at that time, economists were telling us that, economics is not bound by the constitution. Today we have techies telling us that technology is not bound by the constitution and that the constitution has to adapt itself to fit like it did then economics, now techie word.

In each of this there is almost bound to be a certain erosion but it doesn't have to disappear and what we need to do a lot of the time is to shore it up. That's going to be the task. But this constituencies saying that the constitution doesn't apply to them is something we have to frontally attack and destroy.

Q: So, this might be an extension of the IOT question that she raised and like, what happened a few maybe seven to eight months ago in the media was that, a lot of newspapers especially Hindustan Times and Time of India started refusing content to readers because they detected that you had ad blockers. Like I had an ad blocker, so, they started refusing access to me and the argument they raised at that time was that, look, we in the media need to survive which is why it's very important that ads are allowed etcetera and therefore if you had an ad – but what those ads were also doing

was they were tracking my behavior online which is why… So, the question that I am coming to is that, many of our services are getting privatized increasingly. Now in a situation like that private corporations will work for profit as it happens to be the case of the media. They work for profit and therefore they need revenues and so on and so forth. So, in a situation like this, where do, how do I situate my rights to privacy as opposed to their rights to sort of, earn profits or earn revenue from the business that they do? How do I balance and argue against this?

Q: Yeah, and actually a couple of questions I'm trying to collect my thoughts on this because at one level there is individual privacy. At another level you can say there is an organizational privacy or a national privacy. Do they differ? And can the same kind of legal framework apply across? Is there some abstraction that one can do about what information belongs to an individual, an organization or a nation? And who it may be revealed to? Second part is basically in the so called de-duplication of AADHAAR data. Our data has already been shared for not just an individual but the billion people supposedly who went in for an enrolment with unspecified agencies for unspecified time and in unspecified ways. Is that a violation of privacy of the nation not just the individual? And is that something that has a legal framework which can debate and argue and deal with it? And at the level at which the court is now pausing in order to deal with the question of whether this is a fundamental right or not a fundamental right and obviously it seems to have no urgency to determine whether this is a fundamental right. So, the question is, how can this actually be made to come up to argument early enough? Is there a case to be made to point out that this is really a critical issue? Apparently in the minds of these legal luminaries it's not such a critical issue. So, how can it actually rise up to that? So, maybe I'll collect my thoughts about some other questions I have.

Q: Yeah, I just had a quick question. So, neither of you all mentioned the draft privacy bill. So, I'm wondering like if you go through the legislative route, is it better to go through a sectoral framework like you are talking about that draft health bill or whatever or is it better to do an overall thing? And also in the morning there was this, one of the points raised was, is it better to go through a data retention bill or a privacy bill or do you need both and whether you all both had thoughts about that route?

L: So, firstly on internet of things, I agree. I read a very distinct report by the Berkman Center, it was on encryption and it was also stating, I think after the fifth or sixth page

that the entire debate on encryption is skewed because it does not consider that the multiplicity of censors which now surround a person, right? And how much information is taken which is not encrypted. Hence the, going dark, metaphor which is that if your encryption works on your phone for one device, for one application it does not actually secure much, yeah. So, I think that opportunity does arise but for that policy makers, principally government and institutions need to open it up and they are not doing that and they have not done it except the one exercise by the department of personnel and planning, the DOPP approached paper. I don't think so it's been open to us till now to even comment on a privacy law. And I think that's the only form of confidentiality applied to privacy law in India till date, that the law itself is not made available to us.

The second thing is that there a chasm between tech and the legal communities in India? Yes, there is and it's quite sad. There is a greater need to build inter disciplinary capacity as well as trust between both communities. And I think they're indispensible to each other as tech becomes more pervasive in our day to day function. It stops being an on off switch. So, I think engineers are realizing it more and more, there are lawyers who are realizing it more and more and I think there are one or two judges who even now know how to code. I don't but they do. So, I think there is a movement towards it but there has to be a greater sense of cooperation between both rather than seeing law as an inefficiency and as lawyers having contempt for engineers for them not knowing the fancy words that they do which are useless. Okay, I didn't say that.

So, now I'm just wrapping up a couple of them. I have to go on a call, I'm really sorry about this. But private enterprises should be open to do what they want to do but they have to always do that within the bounds of law. They can't make an efficiency argument always. It doesn't work for the environment at least in principle, why should it work for privacy? Of course it's more mediated. It's not an absolute. And that's the function of the welfare state. It has to make those compromises between public welfare, private profit and sometimes they are opposing forces, sometimes they also work together. So, it depends, what's the circumstance right? Probably there are even opportunities for private industry in safeguarding privacy but it has to be seen how they are. There's a very interesting website by the ACLU of California which is saying

and making the case how privacy actually goes towards helping certain businesses. So, I don't know. We probably need to engage with it a little more positively.

In terms of sharing of privacy and where it's going, what's being done already, so, Salmon defined the right being a remedy enforceable by law. And there's no law, there's no remedy, nothing's enforceable. What's gone is gone, let's at least look towards the future. And I think pushing all of this does require an emphasis on the right to privacy as C was saying right now. And as K has illustrated. What may help push the court a little more is what was Siddharth's indication. He was saying probably the legislative route. I think the legislative route does not only build noise per se but it also builds a certain form of political consensus. It does show that it is an actual issue to the courts and it does matter. Of course larger coalitions need to be build between private industry, civil society as well as certain segments of the government for this interest to completely overpower and then for us to get the idealized versions of legal norms that we crave. Thanks that's about it. Thanks. Sorry.

Q: Actually in response to that question about how can we bring this. I'm quite happy they are delaying because I don't think the court has been open enough to privacy because I think they actually have supported it in far too limited a number of areas. And because I don't see the court taking very progressing stances on internet related issues. I think they half of the time don't understand what they are talking about. And the reason we got such a positive judgment in the case 66A was only because there was so much public pressure on it. And that became much easier in that case because the abuse was also so obvious and the media covered it widely and so it was much easier to get outraged across a wide board. And I really think that the reason that judgment because it's also interesting, they covered 66A and the rules under 79. And 110 pages I think are about 66A and some 15 pages about 79. And the verdict on 66A is much stronger than on 79 and 79, I think because of the complexities around it did not come in the public limelight in the same way.

Luckily the substance was related so there was some connection but – so, I think it's really important if we want to have a strong court judgments on this that really also deals with the informational aspects, we need people to get talking about this much more. Which is why I asked that question like, what is the way in to get the court to actually sit up and take notice because I really fear what they are going to say. That's

why I'm happy that they're – like let them take some time because we need to get our act together.

K: No, you are right I mean fortunately or unfortunately because of AADHAAR and because the rise of these big data systems the conversation around privacy has definitely increased. You're seeing, even if people don't see AADHAAR as a privacy invasive or as a privacy intrusion and they offset these concerns by the efficiency gains, at least privacy has become a talking point. I see that maybe it's because I am in the spirit of bubble of the privacy space. But that's what I am observing. With AADHAAR I it's easy to make a privacy argument because of the nature of the project itself. The kind of information that it collects and the duration it stores the information for. And in what I've observed and I've been for a few hearings in the case, it's not that the court has taken these privacy concerns lightly. They have been pretty receptive to the privacy concerns irrespective of the fiasco that happened last year when they referred the question of the fundamental right to privacy. So, I am still hopeful.

Talking about a national right to privacy, under the current legal framework, privacy is still an individual right. So, even apart from the constitutional right to privacy which is of course an individual right, even your modern data protection statutes would, say exist in Europe and other places, that itself, the data subject is always only recognized as a natural person. It's not a right available to organizations or to the nation as a whole. So, at least in terms of the law, there is no concept of an organization's privacy or a nation's privacy so to say.

Q: So, if you were to talk about let's say the databases which protect our sovereignty and democracy are something which have to be protected and private to the nation? So, if you were to consider for a moment that all the databases which protect the democracy and sovereignty of a country are to be private to the nation and not to be shared across the world, is that not a right? Or is that something which should be shared – I mean is there a ground at all or there is no ground and why not?

Q: Or sort of add to it. I think when you're talking about on the lines of a national right to privacy or something in at least the illustrations you give, they – we don't necessarily need to go to the right to privacy to address those concerns. I think we have enough rights when you talk about things, the esoteric concepts and terms of art like sovereignty of the state and security of the state and stuff where we can actually

find grounds to address these issues. So, we don't necessarily need to go to a concept of a national right to privacy. We don't need to go to privacy. This is again one of those things that I think we sometimes use privacy in addressing areas or addressing problems where privacy may not be the best tool to address these things especially when we talk about big data and biases in this communication and stuff.

Q: Yeah, so the reason I raised this – yeah so for example if you were to look at the entire AADHAAR database it has been shared with agencies outside India for de-duplication. So, essentially this database therefore has been modified by agencies outside India to decide who is eligible for being issued an AADHAAR number and who is not and therefore to decide who will get what benefits, entitlements and rights and not. And therefore to decide which constituency can have, can favor certain candidates or parties or not. It is not somebody within India who has actually decided this. So, therefore in a sense, this is an issue in terms of how our democracy and sovereignty have been influenced outside our country. Now, you may not – it's not necessary to call it privacy. But since we are talking about privacy I also want to raise this issue because in some sense there is some information that you may want to actually make public to the world because that will help make sure that human rights are protected. If there is a privacy framework which covers something and prevents human rights from being implemented you have a – it's a double edged sword. So, I want to actually raise the issue about, you know, how do you balance that?

Q: So, in Austria, companies do have the right to privacy and they can protect their trade secrets under the Austrian Privacy Act which is weird because the Austrians effectively extend an individual right to legal persons, I find. But in Austria they fought very hard to have this also included in the general data protection regulation, so, clearly they find it worth to them. Now, normally if the Indian government sends off a database to the abroad in such a way that an Indian citizen is impacted adversely, I would expect that to fall under the right of privacy of the citizen with respect to their government. Like you, as a citizen you have the right to expect that your government does not treat the data in such a way so as to rob you of your rights domestically. So, that would fall under the right to privacy and so far as you have expectations on your government but not to the extent that the government itself enjoys a right to privacy. It has failed you. It is not that the abroad failed your government, your government failed you. I would, with my European framework I would conclude this.

K: I think the other regulatory took that looks at this is, this concept of data localization laws. So, under the AADHAAR act you have a legal requirement that the CIDR, the data inside the identities repository database will always be hosted in India and that data cannot be transferred out. There are a number of reasons why data localizations are problematic but in terms, I mean, but that is the appropriate legal framework under which you can look at it. It's not strictly a privacy framework it's more of a security and national interest framework that data localization laws are – that's the incentive behind it.

Q: She answered what I was – but to try and attempt to answer some of this, I would assume that they were, whenever data is shared, it is shared through agreements or SLA, Service Level Agreements or other which would have confidentiality clauses which would then extend a certain degree of protection to that data. Interestingly in the space that I am currently working in which is critical information infrastructure, it's very interesting to note that the first entity and probably – only two entities have been notified as a protected system under 66A of the act and AADHAAR is the first one which was notified as a protected system. So, enhancing the level of deterrents from it being hacked or modified or changed or anything.

Q: Maybe I am just throwing my confusion here but if we're looking at something like a privacy law or something of that sort then we have to, kind of, I think look at whether privacy is a desirable sort of thing, something like a social good kind of thing. Do you think that privacy is a social good? And if people agree that yes, it is a social good of some sort, then you would have to look at debates about whether – like I don't know too much so, please hang on. Whether it's a negative right kind of thing? Or whether you enable the citizen to have? And then you get into a whole quagmire of negative versus positive and all of that thing but I think it will also be helpful if we can look at it as a social good and what are the things around that?

Q: Sort of just to step back a little bit I just wanted to get a sense of what the room thinks about structurally viewing privacy. So, are we going to talk about by right to privacy, the right to ownership of one zone data? Or is it going to be the fact that the right to not be – data to not be collected about me? So, are there certain facts, like do you want to – so, just generally in my mind these are two structural aspects in which privacy can actually be implemented is, you can either say, don't collect data about me or give me the right to forget or whatever. Or you say that I own the data and by

ownership of that data and thereby the use of companies of – the use of that data by companies will be bound to certain conditions or certain regulations.

So, generally because we are talking about a lot about the right to privacy I'm just thinking about how do you structurally define tools in which you will – like in the act or something like that, how will you define privacy?

Q: So, first of all on the concept of privacy as a public good. There is Fairfield and Engel, Fairfield and Engel wrote a good article about that in Duke Law Journal just earlier this year which I can highly recommend to actually everyone in the room that if you haven't seen it yet you should see it. Fairfield and Engel. It's open and accessible even so it shouldn't be too difficult to find.

Now, that European data protection framework definitely encourages of you of personal data as a kind of ownership right. So, if India in its privacy act goes down the road of data protection almost inevitably with the consent mechanisms and the purpose limitations and all of these things, you will end up in a form of quasi ownership right. And granted in Europe it's definitely not as strong as other immaterial rights like copyright or patents or trademarks but it's going there and it's something that emanates from you that you own and that you can make contracts about with private parties. And then the tricky bit is really in a lot of member states what happens with personal data which is held by the government. I think considerably more governments consider it their property rather than the individual's property than it's actually called for by the law. But that would be a natural consequence of data protection laws I think. And this is in fact also what Fairfield and Engel criticize that because we have this ownership dichotomy in the data protection laws, they are more difficult to create the public to its framework where privacy is seen not to something only pertaining to one individual in individual circumstances but also to groups of people in [Inaudible 13:13] circumstances.

K: Just responding to what you had said about whether privacy should be that you do not collect information or whether the information collection should be subject to certain conditions. I don't think in this day and age it's possible to say that do not collect information about me. That, I think we've crossed that stage. So, the idea has to be that you implement a rights framework which allows you to be in control of that information that is collected. That's what data protection laws across the globe are

doing. So, you regulate information collection, you regulate its storage, you regulate the purposes it's used for, you have notice mechanisms, you have consent mechanisms and you have enforcement mechanisms. So, if all of that doesn't work you have an enforceable right. So, I think that's the idea that we should be…Yeah, the right to opt out is a very important right under data protection itself but there is a difference between how this right can be exercised against the state and how this right can be exercised against private entities. So, there is still an argument to be made that against the government collecting your data for some essential service that it's giving to you, you should have a right to say no. I do not want to share this information but that does not give the government the right to deny that service to you. But that same argument unfortunately there's not enough, I mean, it's not a strong argument when you use that, when you extend it to private entities. So, then the private entities have a reason to say no, and they can deny you a service if you deny them the information. So, there is a slight difference over there.

A: So, I have a slightly different view on this. To sort of begin with your question, I think, first I think it is important to recognize that when we talk of a personal data then data protection frameworks are to a large extent viewed mostly as an end to privacy. So, the right to control one's data is not exactly synonymous to the right to privacy, I think K covered it very well. There are various other aspects which are included in our conception of privacy. When we are talking specifically about personal data, I think at I hold a different view from this room to some extent because I don't think fair information practices or data protection frameworks as they exist currently are very efficient in protecting privacy or providing us any form of meaningful choice. So, whether we move to a right to opt out framework or we have a better privacy notices, I think all of that given the fact that we now live in this age of big data, we are I think we are faced with the scale of data collection that it becomes very, it might be impossible for anyone to have the kind of cognitive capacity to actually exercise that meaningful choice.

Going back to I think the point that you raised earlier about taking a different approach, I think we need all of these protections. It's not that it's in either/or. We need fair information practices, we need privacy to exist as a fundamental right. But I think on the top of that we need possibly, we need to look at risk based assessments, we need to look at harms based approaches which talk of the legitimacy of certain use

cases of the data itself. So, as an individual even if I have given all the permissions, even if I have all the tools and access available to me to withdraw consent and to state that certain use cases are not okay with me, I think even after having all that, I think there needs to be an additional layer of positive obligation on all data collectors. To reach there I think a person needs to articulate what sorts of use cases are legitimate in what contexts. I think there was an earlier point made about data being a commodity and whether data subjects should have a right or some share in the profits of that data, I agree with C that I think that's a very dangerous path to take. What I would like to state there is I think there is, I think big data also often functions in terms of alienating us from our own data. We are instrumental in the generation of data about ourselves and that data is used for purposes which often are detrimental to us. So, some sort of an articulation of a value where, if data is collected from an individual and if a data processor wants to use it for purposes which are not for the benefit of that individual or the individual as a part of the society as a whole, do we look at certain premiums over those use cases? Whether a private party should have to pay for it or look at other obligations placed on them?

So, I think those are important questions when we talk of privacy going forward in the context of big data. And I think the constitutional debate to privacy is obviously very important but I don't think it will address the informational aspects of privacy to a large degree because unfortunately we don't have juries prudence in this country which covers private parties as subjects of fundamental rights processes. So, unlike you we don't recognize them as private rights. The other approach that we could take also something that E covered earlier is to articulate some sort of fundamental rights to data itself. More and more we are, we seem to be moving towards database economy. We are becoming a database state in that sense. So, there is value in thinking about whether there should be a fundamental right to one's own data and what should be the contours of that.

Q: Yeah, my point was a slightly more general point that – when we talk about privacy and a privacy legislation and the general understanding around privacy. I feel that somewhere we're getting too focused on data and we're failing to recognize that there is still a significant amount of information which affects our privacy which cannot be converted into data. For example, the situation in which our privacy cases came about like, Govind– and even Kharak Singh. That wasn't data focused privacy violation. Even

today, if a lot of police surveillance happens on the road while they are following you, there is no data generated there. And we need to make sure that we don't lose sight of that aspect of privacy when we're talking about a privacy bill or the entire conversation about privacy.

C: Yeah. So, that gives you some kind of a framework on how you view these things. The second thing is that a lot of the problem comes not out of just individual databases that have what they collect but also the ability to converge this data. And there has to be some kind of a legal structure which says that you cannot converge the data and you cannot share the data. What we instead have today is no data protection law but we have a data sharing policy. We've really gone the other way. And the third thing is that now we are kind of ready to figure out what our normative framework should be. What kind of doctrines do we adopt? Because we can't do this reactively all the time, we can't do it on the basis of individual cases and – it can't happen like that. We do have a much broader understanding. I think we should start with putting our axioms down. I think it will help us.

A: Also to respond to the point about IOT which was made earlier, I think there is now a lot of study in literature which has been done which talks about how privacy notices should be framed in light of these IOTs. So, I think one of, a very useful study could be done by Florian Schaub. And some of the things that she talks about is, when we are dealing with technology where it is not very easy to access a privacy notice then there are various things that you have to consider. You look at the timing of the notice, you look at the modality in which it is made available to you. There could be auditory visual ways in which privacy notices can be made available or there could be secondary devices with which they always have to be connected in some way. So, there is some articulation of improving the design of privacy notices. However obviously it is going to be much more difficult with the advent of IOTs but I think you might want to just look into that.

C: Just one thing, actually it worries me when I hear things like this that, in this last conversation, I think the poor have completely dropped off and that's really dangerous because a lot of the people who are getting hit are the poor. And we have illiteracy, we have poverty, we have distance and remoteness, we have un-connectedness, we have all kinds of things. And we are also distancing ourselves from it, that's like damn dangerous. So, maybe we stop worrying about IOT and start

worrying about – I mean I'm saying, I don't mean stop worrying but I'm saying give weightage to it.

Q: Can I just say that's, I think that internet of things and these things is entirely relevant to the poor because in fact, perhaps that's a perspective we should be looking at it more often. Solar power projects which gather the data about someone's life and from that you can easily find out their religion and various other aspects about them that then later will turn into the data for micro credits and finance and lending and things like this. If we look at the real harm of these technologies and perhaps the way of the future that's going for the naught, the way things will be going where, when initiatives surrounding using social media for credit and things like that out rhythms, replacing doctors, these things, it's towards the poor that perhaps we should be looking and focusing. And about the privacy notices, I'm just concerned with the amount of things you can learn from internet of things and what the analysis can do in the future and what they're working on with the new analytical techniques. Do you have a privacy notice which says on it that we're going to find out your religion, what time you go to bed, whether you got a mistress, these sorts of things driving from it? It's problematic but you're then past, privacy notices passing the responsibility onto the person involved as well as the other side of it.

Q: So, I just wanted to come back to C and just wanted to flag one thing off which I also felt a little bit. It's that, when we talk about data or individual rights, I respect that. However like I think you said initially today in the morning, we also have to realize that big data or any kind of data is also used for, like, you gave the example pin coding right? Pin coding specific geographical locations and you have that. So, in the sociologist David Lyon's terminology this would be something like surveillance as social sorting. Now in a society which is so unequal where the trouble with big data or one of the troubles could be, I mean it could be used both ways. You can find out specific places that need help and provide help or you can use it in a different way. However in a very unequal society like us in terms of all parameters it is very likely that the privilege will get the benefit of the big data mining or whatever you want to call it and the un-privileged would be reified and their un-privileged or discrimination would become many more profound. So, thoughts would be nice.

Q: So, a quick question, I believe that there is a list of 16 people or 18 people with black money with the Supreme Court in a sealed envelope. And there is supposedly

privacy which is cited by the government for not releasing this. I believe that Ratan Tata has filed a case about the Nira Radia tapes saying that, citing privacy has been violated and there needs to be some framework. In contrast to that we are seeing literally lakhs of people across the country flooding to banks with their Rs. 500 and 1000 notes where their privacy of their income, wealth what have you, has obviously no concern. This information I am told is already linked up with the income tax department. So, every rupee which is, every Rs. 500 note which is deposited above a certain amount is going to be flagged with them. So, obviously when you talk about this big divide between the poor and the rich, in terms of privacy, there seems to be a huge divide and maybe some comments on that.

C: There is one thing that I found it useful to think about these things – every time we say something on the UID project they would say, that is, you're always looking at abuse. And actually that's not true. So, I find that looking at it as intended consequences, unintended consequences and expected consequences that you can expect that. You may not intend it to happen but if you just look at it you can expect that that's what will happen. Then the way in which information is collected, the places where you use coercion, where you say that if you do not I will not or you cannot get or whatever, that has some kind of a framework within which I find it a little easier to understand than I did before. So, I just thought I'd share.

Q: So, I just wanted to make the point about how we possibly need more field ways, ethnography work also to kind of feed into our discussions. For instance, I know that I and her team have been visiting whatever Haryana and western UP for instance around just and some of the questions that she spoke about also come from that right? From speaking. And my colleague B who unfortunately couldn't be here, some of his fieldwork for instance, in his fieldwork he found that many young boys, young men in Rajasthan actually look at Facebook together. They look at the page and they are like, four of them have one account or something. So, even to kind of – not that it means that privacy is less important but the fact is that maybe the way we approach some of these things is slightly different. So, how do we take that? And then there's this Danah Boyd who we've been reading here at [Inaudible 13:18], she's this author in the US and she did this field ethnography work with US teenage girls and to – because there was basically a big scandal that broke out where it was discovered that many teenagers were sending sexually explicit pictures of each other across. Because it's a

crime under US law, they were prosecuted. Then they found out it was so common that it didn't make sense to prosecute.

So, she went and did this study where she talks about how privacy – privacy is important to them although they are sharing the stuffs. So, you know even how do you understand their notion of privacy because you can't just assume that because people are sharing the stuff that they don't talk, that they are not concerned about privacy. So, I feel there needs to be more work also to be done through the field as well.

I: Well just on that, I think on those particular cases, that's again about who young people see as the locus of control right? Because often these image – and this is also a Danah Boyd's work show is that, actually young people don't think sex thing is a stupid thing to do. They think it is a stupid thing to do in a particular context. So, they are very clear about what kind of relationship you should have before you do this to make sure that this does not become a problem. And if you do it in circumstances for example where you do this because you want a guy to get to like you, then you've been an idiot because very clearly in these cases you set yourself up for abuse. The locus of control for most young people is their parents which is also why they are not so worried about governments or corporations or whatever. It is parents and that's where most of their privacy producing behavior or retaining behavior is focused on that. Well on that, feminists approach to technology in Delhi who work with slum adolescent girls in these issues, the executive directive calls Facebook a network of 'bhais'. So, for that reason right? The girls are being surveilled not directly just only by their brother whose phone they're often using to actually access Facebook in the first place but also all of his friends who are all networked on Facebook and all also keep an eye on what girls in their community are doing on Facebook. So, it's a network of 'bhais' for the non Indians that means 'elder brothers'.

Q: Last question. A question for C or anybody who knows, do we have a sense of what's the profile of the people who don't have an AADHAAR yet? Is it mostly upper class or is it mostly poor? Because that speaks also to your point.

C: It's difficult to say what the profile is but this much is clear that more and more people from the classes who see themselves as needing it urgently are finding themselves unable to get onto the database. So, we're meeting a lot of people who as the database has grown when they go in for enrolment find that they are getting a

card. So, it's not like they are not going because they need it. They are not getting their pensions, they are not – so many are falling off like that. That we've met a large number. All the people that we've found like that are poor. There was one person who I met who belongs to the middle classes whose fingerprints didn't work except two. But he got his card but the others have a problem getting on at all. They told that – they don't get any reply at all and when they try and find out they told that it's – you're a duplicate, and like you're already on the database and they are not so, these are the false which exciting who are getting left out.

K: So, on that as well but again no numbers of course but the general sense is that there are handful of social elite who still can function without having AADHAAR number yeah I'm sure there are several in this room so, there is them and then there is – at least there's a god number of not so elite people who are getting stuck with something that Hans Varghese Mathews of CIS has predicted which is that of false positive numbers will be quite high as the database grows so.

Yes, sir, that's right okay sorry, sorry the other comment which is about the discussion that the process happening about discussion of privacy and young women in different context and I thought I talked about this earlier but the discussion was quite a womanly actually which is that privacy has to do something with power and that is something we must keep in mind, yeah? It's really about – so we want to be private in situations where giving away certain information in whatever format that might be that information will get away that giving away this information may come back and affect us negatively if I mean that is really the code of it. If it affects us positively such accepting free services from Google it's not a bad thing really but only when we are aware that Google may have some negative impacts as well, that is the moment when certainly we are aware of a loss of privacy yeah? It's a simple hypothesis really but the point I'm trying to make and I think this kind of a this cultural kind of dimension of privacy where the Indians have a different kind of historical, spiritual kind of understanding of privacy, these kinds of discussion keep I mean keep happening in these circuits. Many people write about it some almost recognize such kind of cultural understanding privacy to support their arguments right?

And my example and I am very happy if more of you actually use such examples, my key example is that of NSS surveys, The National Sample Surveys, it's very well know by all social scientists and people in general that NSS surveys are not really reliable

because in most cases the surveys do not get the right answers even that works for Census but samples surveys are particularly kind of not of reads for not having the right information because people thought that they don't want to give the State the right information because if the State knows the right information it will come back and bite them so, it's not about the point about whether people ask you about your salary when you travelling together in a train, they ask you about that because they want to break the class barrier right? So, they want to create or they ask you about your family whether you have a [Inaudible 3:28] daughter and stuff like that because they want to have a conversation about things that are common to your lives which is beyond your class, caste, identities and so on right? So, that's really not the Indian spiritual understanding of privacy. The Indians spiritual understanding of the privacy is best found in bad quality Indian databases. The bad quality because people are rather aware of what kind of privacy harms may be caused where the State have your good understanding on them.

So, next time anyone tells you that Indian people are different and hence they don't have the same sense of privacy, ask them to work with NSS data and make a real judgment about India because that's a real task.

C: That's you know their interest that's what the collection of statistics Act recognizes. It says that if you give wrong information or misleading information you can be imprisoned and that's because they recognize it because they've got rubbish on the data and like they have rubbish on the AADHAAR database; UID database. There's a reason why we don't say AADHAAR haan we'll tell you that later.

K: Yeah this is just small thing about this particular cultural of privacy in terms of not reporting right data is that many, many times it is also very well thought out political act to reply in certain ways especially to Census data where entire communities have come together to reply in a particular way to a Census Form in order to change categories in particular ways and Census operatives have at time said yes and at times said no, so there is a way in which there is some amount of controls in terms of how the data gets to be categorized or columned but it is precisely the loss of that which then begins to create certain kinds of problem like the 2011 Census to particularly low because it was the first Census on a tab so, the surveys had only the independence to click on certain points on the columns and not write down exact answers which then immediately meant that people took a lot longer at times turned off their survey

because they wanted to put in particular answers to the Census and not simply click on particular parts of the columns that's just -

Q: There's a note on how people also evading the systems or the classic system, classic ways that people know as they either type it in their language so when you communicate instead of you're seeing this Standard English language it's everybody can else can communicate so we have these decoding pattern so, like we have a common language, we use some phrases which only both of us know and this probably extends even to structured data so, in fact I was reading a twit where one person was saying that, "I'm going to S bank and give only a Tamil ID", that has nothing in English so nobody can trace me and even computationally since the Indian computing is lagging and this is not a possibility yet and probably we'll get there but that needs State investment which is probably not anytime coming soon. So, there are ways even in digital world to kind of hide data and be legal.

Q: Also actually by dozen a side I guess but what you were just saying reminded me of some recommendations which is confusing online surveillance also by putting out all kinds of data that like liking things on Facebook that you don't really like. The interested thing is that a little while ago so Facebook has this setting where you can switch off whether they can track you on other sites or not and what I did was I looked at and you can see also what they think are your interest so, I looked at what they are thought on my interest when that thing was on and then I looked at what they thought of interest after I switched it off and it was actually more accurate after I had switched it off so, then I thought now I need to like because clearly like for me to switch that on is partly I guess because I read widely even though I equally don't care about everything right? And so clearly if Facebook is growing conclusions on that bases which are wrong, I thought that's great so basically that means that to confuse them I have to allow them to servile me much more rightly.

Q: I'll just answer your question on the Radia tapes because I had a role in that and as a Organization we are also parted to it or the organization that I was associated with. Now there is very interesting aspects to the Radia Tapes which is very interesting from a surveillance perspective. First of all, surveillance laws allow you to put a person under surveillance only for 60 days after which it has to go back to the monitoring committee. The monitoring committee is supposed to then delve into why the person is under surveillance and then give permission for further surveillance. In her case she

was put under surveillance for 180 days but when the case went to court because of the pressure on all the 2G case and the other cases and so on and so forth and also the court said that you have to establish criminality of the conversation etcetera, first of all, she was not even made an accused by the authorities and they were also – she was just a witness and finally when the CBI examined they came back and said there is no criminality in any of the conversations which of course I wouldn't agree but this raises the first big question that if the monitoring committee allowed her to extend the surveillance on her then on what basis were they doing this because at that review if they didn't find any criminality and the court has not found any criminality in all the 180 days worth of material then why was she put under surveillance? That's the first point, as far as Ratan Tata is concerned, he is making a very interesting argument. He is not seeking privacy against the State. He says that the State has every right to put me under surveillance. He is only saying that whatever the State has taken under surveillance that should not go out to the media and he only wants a limited protection from it going to the media which I think is a very, very dangerous argument because moment you do that in a way you are agreeing and you are endorsing the State to take your information but when somebody finds out some criminality or something that is unethical or something that has overwhelming public good, you don't want that to come out. So, that's – these two twin aspects are very, very interesting I was telling that and I actually went and even had the chat with the then Cabinet Secretary because I was tracking this to find out that why did the monitoring committee and he is the Chair Person of the monitoring committee and at that time Mr. Chandrashekhar told me that look when these people come to us, they only come to us in numbers. They don't come to us with names or etcetera, we have some Samosas or whatever your preference is, we have some coffee and we have a chat and that's it we said go ahead and do it.

So, this is one aspect to it. Now the 2G thing also throws up another very interesting aspect, one of the secretaries of this monitoring committee is the Telecom Secretary, the Union Telecom Secretary, now that Union Telecom Secretary one of them in the 2G case was arrested and put into jail based on some surveillance but what's interesting is some of that he might have allowed to continue as part of the monitoring committee so again this creates a major conflict of interests and that's it.

Now as K has pointed out that there is absolutely zero in fact may be this nuance is very important, the monitoring committee is not supposed to get into legally what led to the surveillance, what facts you have found to allow the justification etcetera? Their understanding or at least the people have spoken to their understanding is, they're only supposed to do check is whether it has been legally allowed which means basically a signature of the Union Home Secretary and that's all. So when –

C: Okay, yesterday at the conference Q made one very nice and interesting intervention on privacy and I've been pleading, begging, going down on my knees and I'm asking him to say it, I'm hoping he will say it now, you're being invited in.

Q: I didn't have any locus standi there to discuss this and I believe people know a lot more but I have – it's been always thrown at us that and especially in a country like India which has very low understanding of privacy because I mean the kind of lifestyles we lead like if I live in a Mumbai Chawl what kind of a privacy do I really have and those cultural issues have created a problem but within that framework even despite that I the – the framework of privacy that has really helped me is mostly from professor Alan Westin's work where he has come up with four postulates to help us understand what privacy really is and he said that why do you need privacy. First and foremost is it endangers your personal autonomy. So, when I talk to corporate about this, the way I look at it and I look at those MBAs and say if your boss is sitting on your head and constantly monitoring everything that you are doing do you think your productivity will go up and everybody says no, no we hate bosses like that and I said that's why you need privacy so, sadly that's when they started understanding that this is – so, basically your personal autonomy is deeply affected and your behavior is affected because somebody is constantly watching Speaker 1: That's why you need privacy. The second is, you also need a lot of opportunities for emotional release, when you are constantly under the glare where is the possibility of having that emotional release? And one example is interrogations. One reason why every understanding of an interrogation is where a lot of light is put on you because they want to put you and imbalance you. You need that privacy for that emotional release which from a society perspective is very, very critical for a society to evolve and unless you don't have that you will never be able to evolve as a society.

Third is you need time for reflection and self evaluation, now if all of you are watching me, it becomes for me as an individual and as a society to honestly evaluate myself.

So, societies as individual and as communities need space and privacy to evaluate how they are progressing, what they're lacking or where are their areas of improvement. Again to give a corporate framework your annual appraisal is supposed to be confidential. It has to be confidential because people want to give you opportunity to appraise yourself honestly and then send your next key responsibility areas for the next year and so on and so forth. If you don't have that then - if you don't have that without the privacy, you'll never be able to evaluate yourself not only as individual but also as a society and therefore the need for privacy and finally this whole thing about sharing confidences and intimacies.

Societies are built on intimacies and the ability to share confidence with each other. The day you take that way you completely break down as a society so, if you don't have that then you also do as meaning as a society so therefore, like this point that was raised about children starting to share private pictures of themselves etcetera they are doing it in the hope and in the belief and not rather in the hope in the belief that it's actually a private communication and they are sharing certain intimacies. It's another thing that either the technology fails or other controls fail but unless and until you don't have – you're not given that space to share these intimacies you are dead as a society and that's why privacy is so, so critical especially to countries like us which is at a certain curve in achieving democracy and strengthening democracy.

Q: Just because that point about privacy is power has been made a few times right, I think that's also really the crux of the matter of like the question you asked earlier about why is no amount of evidence about the failure of AADHAAR ever went off for – and why do poor people fall off in this conversation so easily? I think to get courts to really move on it, to get a broader movement on it, I agree with you K, I also think the awareness about privacy has been increasing in middle classes also but whether we like it or not it is the middle class that genuinely manage to shift policy debates in this country and sadly when it comes to privacy and coming back to that point that was made earlier about middle classes actually stand quite a lot to gain from big data in a way that poor people might not so, we're kind of stuck there you know, and need to find a way to really get to middle classes also to – to see the importance of privacy and then I think the attention for all the other concern that has already been raised and all the evidence that is there of the how may those poor people of India will be taken much more seriously that's really sad but I think it's also true.

N: Thanks a lot to all of you and to SARAI for visiting us and being so kind and allowing us to come to this discussion, this debate, some people were outside and organizing this so, is B who is also not here, thank you all once again, [Inaudible 4:14], work at mostly done by us, one is not exactly done by HCI it's [Inaudible 4:25] into one thing of course initial direction of all research on privacy and big data is available on the website, we will send you in email, it's [Inaudible 4:36] thank you everyone once again to come to this special I'm pretty sure.

Just to say on behalf of SARAI and CIS I wanted to thank everybody and next workshop that we're having is called Lives of Data it's on the 5th, 6th, 7th of January and it's again specifically on some of the theoretical aspects around big data so it's a – you can look it up on the website, I think many of you all will be interested. Also we – there's a big conference on the 10th to 12th December called the Non-Social Sciences Research Network Conference, it happens once in 2, 3 years for anybody who is interested in Law and Humanity issues is happening in the India Habitat Center again you can look up LASSnet, www.lassnet.org for the details of the schedule and so on if you all would like to attend, thank you.