Liveblog on Data Protection Consultation open house Delhi

We're liveblogging the data protection consultation discussion from Delhi. Comments are largely paraphrased. Please read in reverse chronological order.

[and we're done for today]

1533hrs: Naveen, STAR: What we believe is that most of the concerns are rising from the fact that most of the notices are highly complex. That will enable people to consent for allowing the usage of the data. Purpose limitation should be on the basis of what the consumer wants.

1537hrs: Usha Ramanathan: an accusation of rape or murder. If that gets found, or of someone is a witness or a complainant. we need the idea of proximity.

1537hrs: Justice Srikrishna: in a family court, a judge controls the proceedings. All reports are anonymised. Allegations will be there to understand, for posterity. That information is today protected.

1535hrs: You've mentioned the idea of some things that should not be digitised. One thing bothering me is digtisation of courts. When cases can filed, many things get said. Then it results in what it results in. Everything is getting into the digital space. It ahs huge implications for sociology of our country. Many statements are made and meant only for the courtroom. When they become a part of public commons it becomes dangerous.

1530hrs: Kamlesh Bajaj: There have been other judgments re EU GDPR, and talked about personal information on a company register. That should not be erased. Public interest should be larger than personal right in some cases.

1530hrs: Smitha Krishna Prasad, CCG at NLU Delhi: We have very limited comments today. We'd like to point out that any new data protection law would be crucial. We would urge the committee to be open and transparent and add members (civil society). This consultation in Delhi was with short notice, and before the deadline for the written submissions. We wanted to suggest more consultations, and with adequate notice. Consultations should be after the written submissions. The law commission has used this as well.

1528hrs: Usha Ramanathan: The data controllers liability should be even higher. It's more confusing regarding UIDAI because they decide.

1522hrs: [I made a point about confusion regarding ownership of data, and data as a right and data as a property]

1520hrs: We can look at a BCCC and the MIB, and the BCCC can ask for act

1511hrs: Raman Chima: The ATG has a right to access your data, when the challenges were made to DPAs. Matt Schrems case. The right to access your data must be in the regulatory regime. You can build on top of that as well.

Tehre's a basic to be able to access your data as a basic right. That should be subject to oversight, and right to make it portable, and a citizen focused right.

1514hrs: Nachiket: With regards to Aadhaar and RTI. The composition of the committee is a concern are on public record have made statements for Aadhar. and I would urge chairperson to get some balance by bringing in members of civil society. If we can have an additional round after the submissions, and a second round of consultations. I would like to share my personal experience with Aadhaar: I had to take an Aadhaar before the Aadhaar act was passed to register my marriage. No consent was taken from me. Subsequently when I've tried to revoke consent, which they state is possible, Ive not been able to do it at the center or at the call center. In terms of how this will affect the Aadhaar act or IT act, some change needs to be made to bring grienvance redressal.

From the point of view of RTI, an RTI was filed for the deliverations of the commiteee and meetings, I would request that the committee adhere to the highest standards of transparency.

1511hrs: Srinivas: I'm interested in predictive policing. Algorithms that are governing us need to be transparent and procedures need to be transparent.

1510hrs: Arghya Sengupta: you could stop any process which is automated. Second [missed this]. Third is that you have the right to know the algorithms.

1508hrs:Ajay Bhushan Pandey: What is the criteria a credit rating agency use? Tehre should be some adjudication and review. In some countries, it's not the monopoly of one company. The agency which does this fairly will survive, without disclosing the intellectual property.

1507hrs: Justice Srikrishna: If a traffic camera does this, then challenge it. A judge will ask for transparency. If you expect transparency in algorithms everywhere, then that won't work. The right thing to do is to go to an adjudicator.

1505hrs: Algorithms are discriminatory, but we don't know what governs them. The scoring systems for different insurnace agents, I should have, as a citizen, have every right to know how these systems are designed. Especially inside the government. There are cases where police departments are using algorithms, but we have no idea. These are black boxes. Citizens should have a right to know what algorithms are governing us.

1505hrs: Justice Srikrishna: Fines have to be proportionate to the abiltiy of the data controller, and be preventive.

1501hrs: Ambar Sinha, CIS: It would be worthwile for us to look at the international experience of DPAs and ICOs in tother countries. The UK office has used fines for enforcement. They've realised that wehre data controllers are putting in mitigation strategies, the fines need to be reduced. It's important in the legislation to empower the data protection authority. The powers have to be across a wide spectrum. The authority should have the power to receive complaints, and enforce based on orders that it passes. When it looks

at the pyramid of supports, whether it has privacy shields and trust marks, and carrying out audits of data controllers.

The other point: as far as the principles should be very very clearly in the primary legislation. When specific practices in sectors are concerned, there needs to be active participation from civil society and academia. It took the GDPR 10 years. In Netherlands, it ook them 15 years to come up with sectoral codes. The DPAs should work with civil society and academia.

1458hrs: Ajay Bhushan Pandey: The liability should be proportionate to the damage done. If you look at the cost of the insurance. There will be some other company who will be more efficient and his cost of insurance will be much lower. A good driver will get insurance at a lower cost vs someone who is not a good driver.

1457hrs: Pankaj, Telenor: How will we define liability? If we have insurance then that increases the cost of doing business.

1454hrs: Justice Srikrishna: Take Bhopal tragedy, Uphaar tragedy. If there is a situation where extremely sensitive things are being handled, accountability has ot be higher and there has to be proportionate liability. I'm not talkimg about criminal negligence. I'm talking about civil liability, and compensation. If there is a damage to the data subject, why is he or she not entitled to the compensation. That will be proportionate to the lack of accountabilty of the data controller. The approach can be insure yourself. Why cant this be an alternate way. I agree with Mrs Ramanathan, the law should be person centric.

1453hrs: Pankaj, Telenor: The right to edit and portailibty. We cant have a free for all here since there will be a huge cost. There has to be a fee mechanism. Something that needs to be there. On accountability of data controllers, accountability is required. There will be just lots of categories of data controllers around. the moment you talk about accountability, you'll go to liablity, and the case which is given in the consultation paper, then any data controllers will survive. These issues need to be delberated. There needs to be a limited liability defined.

1451hrs: Justice Srikrishna: What will be the adjudicating process? I'm telling you there needs to be a separate adjudication body. Fro example, stock exchange rules require trade defaults to be arbitrated by members. That's a better mechanism than a lok adalat.

1427hrs: Kamlesh Bajaj: Awareness creation is a massive exercise. Who will implement privacy programs in organisations. The key point has to be that the ombudsman, working with SROs. It would be verticals like DSCI in the IT industry, in banking it could be IBA. The way privacy laws were created, they were codes of practice were created by industry and then it became law.

[He talks about consumer court not working]

1426hrs: [I made a point about right to be forgotten, that it shouldn't be used

for censorship]

1439hrs: Should be independent. You want to make it partially transparent, have a criteria. I'll save this for submissions

1439hrs: Arghya Sengupta: how should public defenders be appointed?

1438hrs: Ramanjit Singh Chima: Seeing the sort of requests that are sent to LEA, there's a safeguard that is urgently required. Sometimes the home secretary is a buffer. Today a tech company has fewer protections than a telecom company.

1437hrs: Justice Srikrishna: Justice Srikrishna: In this country we've had stringent laws like TADA. But there were also preventive detention laws. What were the safeguards provided? There was post facto scrunity. Would it be feasible to have pre-action scrunity by a body put together, a committee.

1433hrs: Ramanjit Singh Chima, Access Now: The FISA process doesn't say that there's a blanked exception for the government. California has a data protection regime. For law enforcement a separate regime applies in terms of what a FISA court can do.

The flaw in the process was that there wasn't a public defender. There needs to be someone saying that this may not be accurate that goes on record. IF there's a process of judicial process, we need a public defender. The UK passed a law that you can challenge a legal surveillance, and it has now said that certain warrants need to judicial approval. The EU court of justice has struck down data retention laws. There should be no blanket security exceptions. It's on the commitee whether you want to put in a surveillance chapter.

1431hrs:

Justice Srikrishna: Have you look at the FISA court option? Do you think it would work if we had a situation where however agent the matter is, it has to be adjudicated by a judicial authority.

Usha: A secret court with secret orders is ineffective.

Justice Srikrishna: Let there be a judge at the rank of an SC judge?

Usha: It's more important to place it on record and there being a review, because someone who makes a wrong call can be held accountable.

1424hrs: Usha Ramanathan: one is where the state is treating all the data and our bodies. The eminent domain principle is also used to hand it over of private players. The other is
The third is national security, which is a type of immunities. In the AP shah committee report we struggled with national security. NAT GRID was supposed to be a pipeline. Then there was a presentation made to the cabinet, and the RTI was that it was about the project. It was delayed for 20-25 ays and then they said that it was a national security exception. All these agencies aren't just

beyond the law but also beyond parliamentary control. You need to identify a legal regime and a supervisory and accountability regime.

1425hrs: Justice Srikrishna: who determines national security? it's the executive. How does one neutralise the difficulty if the person at the top

1418hrs: Usha Ramanathan: I'm forced to come in when there's a statement like no law until we innovate. WE have a lot of experience when we look at the state resident data hubs. It's not about collecting what we want and keeping it safe. GSTN is also in private hands now. There is this ambition of using technology and creating wealth, about a trickle up philosophy of economics. It's appalling that people make this kind of statement. We don't need to assist in this trickle up. We have inequality growing, but now you're looking at trickle up, and to let people monietize this information. The RTI community has been very concerned. They're been asking for transparency. There's a distinction between state being transparent to people and people being transparent with state. We see this committee being constituted by people who support the UID project, and in the report we see

two of your members, we've had seen people arguing that privacy is not a fundamental right and arguing about it. The AP Shah committee was civil society. We would like for a committee to be credible, and for the report to be acceptable.

Yesterday when we had the massive breach of the UID database. It could be any database. It's unwise to bank only on those punishing those who misuse it. If the data controller has to be responsible and the data controller is responsible for deciding who is responsible. That should be avoided. These are things that you should keep out of any framework. Take lessons from what has happened. Yesterdays breach deserves a close study.

On the right to be forgotten, the point about what is happening now, is that technology makes many things possible that we want and do not want. when we don't want it, the idea of opting out becomes more complicated should be. These databases talk across time and across people and various kinds of activities. They leave no space for people to leave their past behind.

When we look at eminent domain. Data is entering the region of eminent domain. I'm not comfortable with my data entering the property domain, and it becomes property. The doctrine of eminent domain is entering the domain of data.

1415hrs: Mahesh Uppal, telecom consultant: I beleive that in a sector such as this, and the scale of innovation, it would be extremely risky to lay down rigid positions. It's important that there's the issue of the data protection authority. Once we have that, if its driven by principle rather than detail, then it becomes incumbent that we have an authority. That would allow us to anticipate what happens in the future. Too detailed a legislation would be counter productive, not only for reasons of scale and innovation, but also it is dependent on assumptions made. These are all relatively difficult to establish,

and there's no way to argue, that just because something is localised in India, does it become more secure? Are we convinced taht localised is secure, or something that is not localised is insecure. We must be driven by evidence of harm.

1410hrs: Praneet, TCS: [Missed most of his comments].

On data localisation, we should encourage data localisation, but we should allow cross border data flows.

GDPR can be a bit vague when it comes to right to be forgotten.

Data controller should be completely accountable. If there's a joint data controller, then there should be joint responsibility.

1406hrs: Apar Gupta: What should be the ambit of the statute and the power of the regulator. The TRAI as a regulator was able to fulfil the public interest in case of net neutrality. What is essential is to define common principles which should be enforced by the regulator: necessity and proportionality. With respect to mass surveillance, there are principles from Justice Nariman. Does PUCL standard hold well and good? We need a heightened standards, but what we need are principles first.

After comments, please have a counter comment period, and comments, and a consultation in person should be held.

1401hrs: Srinivas Kodali: When you've classified only personal data and sensitive data in the paper, but some things are sensitive even in public data. Public data: you don't want your name to be in public records. When you're looking into those it's important that classification of data is done. Is FIR a public record? Can I monetize an FIR as a public record? It's important to look at various kinds of datasets, and not just personal data and sensitive data. You need all sorts of data, and you can build it on public data which is respecting privacy. The distinction needs to be made based on what types of datasets are public. When you're taking about exceptions, you're taking about them in sectors, like for journalists. Data needs to be minimised in a public record, but it cant be minimised in terms of purpose limitation.

You haven't looked at the ownership of data. The paper doesn't do any justice to that. There's also the section on right to data portability. It recommends that machine readable formats for data. What we need is data standards. The paper doesn't talk about encryption. If you're taking about data protection, where unsecure channels are being used, that is not viable if you're not talking about encryption when you're talking about data protection. Without encryption, surveillance by state and non state actors is possible.

1358hrs: Roshan Agarwal: These things started with aadhaar. India is supposed to be an IT superpower. However it gets a fraction of the revenue. Regulate only what is needed. Stick to Aadhaar. Also should have had this paper in two languages.

1349hrs: Kiran Jonnalagadda: I want to look at a few things said. One is data minimisation. People are aware that data data minimisation is good for them. One example is VPN, which comes with no data collection. People are choosing to use VPNs because they dont trust their internet connection.

Secondly, on data anonymisation. PEople say taht anonymised data is safe to share, but it is not because it still shows statistical patterns. Apple has been experimenting with differential privacy and there are challenges. You need regulation on top of good technology.

When you do credit card payments, you have 2FA. The point is that the website that you do it on, it doesn't see your OTP. When you do it inside the app, if it reads the OTP and adds it to the app, it compromises the 2FA. There is simply no protection afforded. The Maadhaar app has time based OTP, but it issues the OTP secret through an insecure channel. Any good TOTP implementation doesn't happen over the air. Technology companies work their way around but operate on a good-faith basis. Regulation should take that a little more seriously.

There has been a statement made that consent is broken, and we should do away with it. This is a fallacy. Software licensing is complicated, and between developers the most promising things that came out was the open source movement. Which was about formalisisng the licensing for software between developers. There's an open source repository OSI, which maintain a repository of licenses. Another example is 15 years ago an idea of licensing for content was in creative commons. It has a simple explanation, and the summary should be good enough. This is how consent should be done. Can there be a standard short code backed by a document that you can trust. That's how you restore consent.

1345hrs: Good to see that the data protection law, as per the paper will apply to government as well. [missed the second point]. Apart from consent, which should continue hopefully, the other five basis in the white paper are reasonable and are worth adopting. We should also differetniate between the data controller and data processor. Lastly we should look at creating positive incentives for data controllers. For example, in certain jurisdictions there is an exception regarding data breach notice to data subjects. They have an onus to report it to the data regulator, not the data subjects.

There was regulation that created 2FA which was on a web browser. The browser enforces boundaries between websites. On a mobile the boundary doesn't exist. One thing that google has started doing is that it's offering a VPN for free, along with Google Fi. Operating system makers have started the importance of VPN. IoS also now allows VPNs. Platforms have started understanding that VPNs are important for users.

1243hrs: Ramajit Singh Chima, Access Now: Anyone who tells you that a global framework doesn't drive what product managers do is lying. The GDPR has forced people to engage with this topic, and the number of studies commissioned

to discredit it shows how impactful it is. There is a set of global principles on privacy.

Do's and donts: [We'll add this later after checking with Raman. He speaks very fast]

Puttaswamy judgment has focused on people and not data. Learn the lessons from the TRAI on regulatory powers. Tries conducts a consultation for everything it does. If there is a privacy commission, it should be for creation for regulation, not enforcement.

There is a problem about data being misused.

TrustID allows people to create profiles of people based on aadhaar information. Innovation is important but some forms of innovation are not acceptable. There are examples even in AI where there are forms of activity that are not allowed. Deep Mind was fined.

1239hrs: Ashutosh, ASSOCHAM: We are at the cusp of a position where we can be seen as the leaders of becoming the data analysts to the world. India today has all the three types of economies: really advanced, developing and the underserved. If we can innovate and create for these three, then we can innovate for the rest of the world. WE need a regime that builds trust in our country, we will create jobs, income. There shouldn't be a regulator but an ombudsman. We're not just talking about the IT industry, and privacy will impact all industries so we need a common framework.

On data flow, law enforcement access and data security, the security of data in a cloud first environment, is not dependent on where the data is. There are checks and balances which are in place, and tehre needs to be an accountability framework. Data localisation and residency were not the first point and were later addressed, and we need to see how we can become the leaders in data analysis. there could be a gradation in terms of things like national security etc.

1232hrs: Debashish, Broadband India Forum: Any curbs on data will hurt the country more rather than benefit the country. What is data processing about? Who is it benefiting? India is talking about having a 3 trillion dollar digital economy by 2022. The point we're making is what is driving this digital economy, and thus any curbs on data collection and usage will harm the economy more. Who is it hurting if we could artificial curbs? let us not put ex ante curbs. If there are any noted harms that are evident then they should be regulation in place to make sure that those grievances are redressed, and the harms should have a redressal mechanism.

21st century is about IoT, cloud, M2M, big data, we believe India has the potential to leapfrog what has been done in the traditional IT industry. We can become the global knowledge hub, by undergoing rapid socioeconomic transformation fuelled by data innovation. Data is not restricted by boundaries. You cannot have India innovation and a china innovation. You need to have exchange of data. You need to be able to make innovation and utilise innovation

for public good. For data localisation, the IT industry would not have survived it. We should allow cross border data flows, and we recommend no restrictions on cross border data flows.

Regulation is good, but regulation for the sake of perceived harms and threats is not the right way to go. Give them the freedom but with broad overarching principles. Industry is conscious that if they harm the customer, and they work in a self regulated environment. Because they are all good responsible entities.

Companies are operating in an environment where they understand the implications of causing harm, so we suggest a framework about preventing harm, rather than providing restrictive principles of preventing harms.

1231hrs: Justice Srikrishna: should the law prescribe classification, or should this be delegated legislation? Should parliament look into it?

1229hrs: Ravi Gupta from NIC: Create classification for what kind of data can be provided or displayed prominently, and classify.

1228hrs: Justice Srikrishna: if constitution is not in 23 different languages, how will you prescribe by law that privacy policies should be in regional languages?

1223hrs: Arjun from SFLC.in: I wanted to address the point about notice and consent, and that we shouldn't do away with it. Notice and consent has not become obsolete. What has become obsolete is the legal form. It becomes a technicality. A number of steps can be taken to ensure that it is procured in a meaningful manner, by having privacy policies in a simpler manner. For this purpose, this should come with minimum standard disclosures, and disclose things that should be collected, what will it be used for, how long it will be retained, and how can you revoke consent. All of these information displayed by default then his will help in a big way to ensure that the consent is meaningful. In the context of the Indian situation, it becomes a problem for people to understand what these policies say, so using regional languages would help.

1220hrs: Rahul Sharma: If we form a law which becomes a non starter for startups, it will have an impact on our economy. We need to be careful about direct and indirect impact on the economy. India's outsourcing business have grown because of cross border data flows. We have to assess our situation. We don't have to consider EU GDPR as a gold standard. They've had discussions for 10 years. The final draft of 2016 is very different what the law for 2012 was. We need to look at how they started. The EU GDPR is more of a handle for imposing penalties on google and facebook.

[I spoke for a bit, pushing for data minimisation and purpose limitation, and addressed a few questions from Justice Srikrishna]

1207 hrs: Usha Ramanathan: I think a basic principle in data protection is that it is not about protecting data but protecting people. Taht's the fundamental principle. I don't think we should go around US route, because that's giving us

innovation but its also giving us monster. It's also important that a lot of what we're talking about data out, or resources.

I found the white paper disappointing because it didn't seemto be taking into account the problems and situation, and changing in the constitutional understanding of what people are. People have said that privacy and law should should wait until innovation is over, and should not impl

1204hrs: Kamlesh Bajaj, individual capacity: On data minimisation: the question on data collection is that should it be restricted in the first instance. The key point is that if we restrict data in the beginning, what are we achieving, we're talking in the context of innovation. The key point is on preventing misuse and harm. To my mind, data minimisation has the potential of harming innovation in the country. We've just started with AI, IoT, and if we put a condition which will harm innovation in the country, startups which need data, or innovation on drones, traffic control, we dont know which way this will go.

On adequacy test on EU GDPR, it doesnt serve any purpose. We've always treated this as a non tariff barrier. it doesnt increase or enhance security or privacy.

1230hrs: [Someone]: we need to incentivise data localisation not force it. We're living in the era of virtualisation, we will lose business if there is localisation.

TRAI has gone the MLATS path for law enforcement considerations.

11:59pm: Venkatesh from DSA: If we accept the accountability principles in our framework, we can… [sorry couldn't get his point]

11.59pm: Arghya Sengupta: On legitimate interest, do you think that this is a balancing test that we can leave to every single data controller in India?

11.48pm: Venkatesh from DSA: DSA urges that outside of consent there are other legal basis for processing data, including contractual obligations, compliance with legal obligations. To go into one extra level of detail, the question of what constitutes legitimate interest, and when you're taking about data controllers taking onus of the data they're taking. Whether legitimate interest constitutes intervening in individual rights. That's one part that I wanted to mention, that there are other legal grounds for processing.

The white paper points towards click fatigue. We believe implied consent could come in to relief some of this burden. this could be an area where the framework could focus on. For example, when you go through a turnstile at a metro station, you're giving consent. Wrt childrens consent, the age that we're proposing is 13, which is lower than GDPR and complies with US.

Consistent with our views of consent, we should have context for data processing when it comes to notice. Notice should support choices that are contextual. The number of devices that we use to access the same apps are increasing, and it could be complicated if we're looking at click fatigue based consent. One

suggestion could be outside of having consent int he device as well. Where you have a public place where you put the notice, outside of the device.

On data scorecard and consent dashboard, some of those frameworks have not been understood well enough. We caution against a consent dashboard. The reason being that as you see technology increase, and prescription could prove unworthy of the decision that you took.

11.38 pm: Amber Sinha, CIS:

We require a strong data protection authority, market incentives for data controllers to comply, vigilant and active citizenry and security enhancing technologies.

On consent, points have been made about consent fatigue. The puttaswamy judgment places informed consent at the centre of any data protection regulation. It would be unwise to hedge our bets only on informed consent. We need practices which would be termed paternal, but they're required for protection of citizens. We will empower the data subject, and he is expected exercise rational choice, but there is information o indicate that that doesn't happen. If we recognise that privacy is a social good, and we hold data minimisation dear, then entirely relying on notice and consent is not absolute. Especially when it comes to sensitive personal data, a risk and harms approach on top of notice and consent would be important. The nature of the consent needs to be clearly set out. The consent has to be freely given, informed and unambiguous. It has to be given as an express and affirmative act. Consent should not be a tool for coercion. When someone is being denied access to service because you don't want to give access to incidental data, we need to check if we rely on market forces. If the legislation sets out a clearly set of rights, that would be helpful.

On data localisation, I agree with what Apar and (karthik from Nishit Desai) said. Data vocalises also has various shaded. One form is that we mandate it exists in our jurisdiction, it would be exported but with a copy, and also where it can be exported without a copy. It's important that it travels with the same protections when it goes outside India. We would look at adequacy and safe harbour mechanisms.

Finally, I would like to make the point that what the white paper does not delve into in suffient detail is surveillance practices, and grounds for surveillance. Given the kind of technology given to us, and the PUCL judgment, it should be important to check how surveillance can be regulated, and also regulation of surveillance will require the state to document its own surveillance practices. These are issues which require urgent attention.

11.36 pm: Justice Srikrishna: If you're doing business in 20 countries, can you say that you will not comply with the laws of that country? maybe some day there will be a global concept, but to start with, your suggestion seems to be that all localisation is wrt govt data, and wrt private data, there should be cross border flow without restriction unless there are security issues.

There is a link between consent and purpose limitation. In some cases even when consent is provided, and if there is evidence to suggest that it cant be acted upon in public interest. Consent should not be an immunity from liability.

11.33 pm: Pankaj Sharma, Telenor: as telecom industry, we've faced this quite a lot. This has been one of the first hurdles. The current rules are, and led by security agencies, are about data localisation. That you cant monitor something outside our borders. The reason for issuing these issues is that there is no global framework for data and privacy. We need to move in that particular direction. How can any country apply a law that is not applicable in their country.

The moment you say the server has to be in India, the global aspects of efficiency will go away.

11.32 pm: Shruti Rao from Information Industry Technology Council: We'd like to opt for a globally interoperable regime. There need to be global voluntary standards. We emphasise that there should be no data localisation

11.30 pm: Kartik Maheshwari: on data localisation, when there are arguments for stored in India, the criteria for empanelment for Meghraj, the govt data is being stored in India. The interests of data subjects and industry are exclusive.

11.27 pm: Smriti Parasheera, NIPFP: data protection is also about your day to day dealings with your eployer and university, and not just big data. The calls for abandoning consent shouldn't be there. There are really are contexts where consent can work quite effectively. For people who say there is consent fatigue: yes there is, and it has become difficult. Just as tech has made consent difficult, it also holds the solution for it. Then the idea of privacy by design needs to be talked about. There is no one size fits all, and we need a graded approach. The role of data protection agency and agency design is important.

There should be a principles levels approach at the level of a primary law, and have a strong enforcement framework for all of this.

11.24pm: Apar Gupta: The committee in the white paper has noted the work of professor anupam chander, his basic rationale against data localisation is that user interest and business are not fully satisfied and give govts more censorship control, and create barriers for business and users from availing services. Countries which have harsh data localisation laws are China and Russia. his work argues against it. I would argue against data localisation. There are several rationales for user interests. For business interests, a large part of the data localisation push comes from Indian industry, which wants to erect competitive barriers.

11.20pm: Shagufta Kamran: Internationally, there are frameworks like OECD which provide good guidance around cross border data flows, and harmonising with them would be useful. Too much prescription will not go in the favour of the industry. Self regulation should be the regime. If we encourage data localisation, it will be disastrous in case of natural calamities. Allow cross border data flows. In terms of the multiplicity of actors involved: there are a lot

of allied laws. The point is how far are we incorporating the necessary changes in those laws as well.

Data as a concept, or a basic principle applies to various sectors. We need to start engaging with the automobile sector and other sectors, who are in possession of that data. There needs ot be a distinction made between data processors and data controllers. That's best governed by contractual laws.

11.18pm: Pavan Goel, individual: The public conversation has been around Aadhaar, but there is private data owned by google and facebook, and this data is stored in the United States. The US laws provide privacy guarantees only to US citizens. These services either willingly or under a US court order violate Indian citizens privacy. Our law may be against that but it will be in conformance with the country where it is. One solution: it's necessary for this entity to have an Indian entity. In order to reconcile jurisdictional issues we should have data in India, and only allow cross border data flows which allow data access.

11.12pm: Pankaj Sharma, Telenor: The team who wrote the paper needs to be commended. What we need to understand here is that as India, we are the cusp of a digital economy. We are looking at questions which are really framed with the right intent, we could have a good regulation, but we could have a disaster for digital India. We should discuss this question by question.

On notices and consent is that consent fatigue is already there. I dont think anyone reads it, whether us or anyone else. What happens is that the aspect of having the facility is taken more than privacy. We say yes to everything. What are we going to incorporate which is going to matter. We need a simple law with protection, and the notice says as long as whatever is happening is being covered by the data privacy law of India, it should be okay. We can't have lengthy consent. If you're taking about privacy law, the paper says that there are two types of data which can be used: anonymised and pseudonimised. Then consent part does down. When do I need to share my data? Or the portaibility of data. These issues come when I'm interested in sharing that data. As a data controller I want to use the data or as a consumer I want to share my data. If they can use anonymised and pseudonimised data, no consent is required. For medical records, we can have a stricter law. Even for Aadhaar there is an OTP based system. I could say okay on biometric based system.

For Children, it has to be over parental guidance, and that age could be just 15 years.

1110pm: Charu Malhotra Indian institute of public administration: This is less about data and more about people. Data protection has two aspects: the privacy issue and second is commercial issues. I did not find clarity on the remedial action in case it is breaches, in case a company breaches data protection for the masses. Let citizens be partners in crime in case of commercial aspects of data. Why aren't we able to think of a dashbord scenario, if I give informed consent

then I know where data is given in the pipeline, and what is my percentage share of it.

1109: Sharad from institute of company secretaries: About medical records, it's sensitive information for patients but important for regulating the medical profession. How to balance this, because the data has to be provided for competition, but sensitive parts could be taken care but also competition is taken care. Balance has to be maintained, it should be portable, available for research as well.

1105: Ujjwal Kumar from CUTS International: Data protection isn't just necessary from data protection, but also from competition point of view. The right to data portability is something I want to flag as an issue. Every economy follows its own rules and philosophy. Data portability needs to be upfront as a principle, because it goes beyond privacy. The right to data portability depends on the definition of personal data. The larger principles should also include the consumer usage data, allowing them to be portable to help increase competition.

1103: Gopalakrishnan S: Topics for discussion:

- How can notice and choice be incorporated in a data protection law to operationalize consent? How can children's personal data be effectively protected?
- How should "data localisation" and "cross border transfer of data" be dealt with under a data protection law?
- What should be the nature and scope of the possible exemptions under a data protection law in the Indian context?
- What are the different types of individual rights, their nature and scope which can be incorporated in a data protection law?
- What are the different types of individual rights, their nature and scope which can be incorporated in a data protection law?
- To what extent should data controllers be held accountable under a data protection legal regime?
- What will be the impact of a data protection law on allied laws, particularly, the Information Technology Act, 2000, Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and Right to Information Act, 2005?

1101: Justice Srikrishna: We're here to ensure that the data protection law, which has been the buzz word in the country, becomes crystallised, and the inputs that are necessary to crystallise it are taken forward. An opportunity has to be given to stakeholders what their concerns are so that they can be noted and addressed.

If you point out a flaw, I'll say what is your solution to your problem. I want solutions from you. We'll note what is wrong, and set it right.