Notes from Srikrishna Committee open house in Mumbai

We tried to liveblog the data protection committee consultation in Mumbai yesterday, but Internet connectivity at IIT Bombay was pretty poor. Below are the comments that we were able to note down: these may somewhat paraphrased, often exact, but shouldn't be treated as a verbatim transcript. We missed some bits, and skipped some comments, which we either didn't get, or were repetitive, or when I was commenting. We've identified speakers wherever possible.

Also, I reached some 15 minutes late, so only caught a part of some great opening remarks from Dr Anupam Saraph, which haven't been included below. Two fun parts: firstly, a person from Hindustan Unilever saying that he's speaking in his personal capacity, and then going on to make a company specific comment. Secondly, an ICICI Bank representative trying to justify buying personal data from clubs etc and using that for marketing (i.e. spamming). Go figure. Anyway, here are the notes from yesterday:

> Update: Anupam Saraph send us an email with the points he had made, which he shared with Justice Srikrishna as a letter. Here's a summary:
>
> **# Is data protection technology centric?**
>
> Data protection cannot be the protection of data in a particular medium like digital. We cannot create a data divide by restricting to the digital. We cannot borrow technology ideas either. For example eKYC is not KYC. KYC is not reusable as eKYC is. There is no identification in authentication. We are creating a legal mess by using authentication where identification should have happened and we assume it has happened by authenticating biometrics. We cannot automate business process without preserving original responsibilities. For example the branch manager used to be liable for account opening and creation. Now no one is.
>
> **# Who is the beneficiary of data protection? Who do we protect and from whom?**
>
> The people whose affairs generate the data when they engage in a, legal, common purpose must be the beneficiaries of a data protection framework. For instance the banker and customer come together for a common purpose. Similarly the citizen and the PDS come together for a common purpose.
>
> The beneficiaries *cannot* be third parties who seek profit from data of systems they have no role in, share no common purpose with the parties whose affairs generated it, and do not have any skin in the game to protect the parties whose activities generated it. For example,the data of the banks and their customer or the citizen and

the PDS are not generated for third parties who have no role or skin in the game to further the common purposes of those in the system.

If we fail to keep away third parties, they will colonize, corrupt or destroy those systems whose activities resulted in the data.

For instance: Neither the UIDAI nor its "ecosystem" have any role in the affairs of the people who have come together in different systems to further their common purposes—from enabling borrowing and lending money, enabling ability to connect and communicate with others, obtaining education, ensuring ability to travel abroad, to ensuring food security, or even to get a dignified burial. UIDAI has no understanding or role in the common purposes nor does it protect or further the common purposes. It has no skin in the game. This overreach destroys the symbiosis between the borrower and lender, the mobile user and service provider, the passport issuer and traveller, the hungry and the food provider. Along with the UIDAI, the GSTN and the NPCI, for example, are similar third parties that seek to profit from data of systems in which they do not share any common purpose with the participants of the system. All of these demonstrate how third parties have colonized, corrupted and are destroying systems that worked well before the intervention of the third parties.

 # What is the purpose of data protection?

In end analysis data must be protected because it furthers the affairs of the people whose affairs generated it; it is protected to ensure their affairs are just, free of inequality, free of indignity and do not destroy their liberty. After all furthering the promise of the Preamble to the Indian Constitution is fundamental in governance.

 # What should be the scope of data protection?

There is nothing more important to those in any system other than empowering their common purposes. In the process of pursuing the activities towards the common purpose in any system, data is generated, certified, authenticated, updated and also restricted from use by third parties. It is also audited to increase confidence in the protection of the data throughout its life cycle.

For example the delivery of rations the generation of data, its certification, authentication, updation and restriction cannot be unequally or unfairly regulated by one participant or an outsourced agency without skin in the game to serve the purpose of ensuring no person is denied rations on first visit.

The scope of data protection framework cannot, therefore, restrict itself to privacy or restriction of data access. Privacy does not protect the parties engaged in common purposes unless the entire data life

cycle is dealt with. In fact data restriction is not just about privacy but also about data sharing.

Furthermore a data protection framework cannot restrict itself to digital and create a data divide. Any data protection framework should as much protect the non-digital as the digital. The Constitution is not about the digital or data economy, it is after all about ensuring justice, equality, liberty and dignity.

 # What are the principles of data protection?

Data Protection framework needs to protect Indians to ensure at least minimum protections. Here is just an indicative list of the protections that the Framework will need to ensure.

• Protection principles have to be based on the objective to ensure justice, dignity, equality and liberty of those whose engaging in common purposes results in the data that is required for the functioning of their systems.

• Protection must ensure that the protection of databases that protect the sovereign, democratic and republic status of the country.

• Protection must include the protection of the manner of creating the data, certifying it, authenticating its copy, restricting its use, auditing its creation, certification, restriction, updation as well as ensuring its fidelity and updating it.

• Protection from coercion of any party to need to participate in any scheme in order to create, obtain or use data, that forces digital, includes parties without any skin in the common purpose of the system generating the data, exceeds in scope, or is contrary to the common purpose of the system they participate in.

The Economic Times recently ran the story of all of India's Electoral Roll with 68 attributes of each voter for every constituency being offered for a price by an American company. This indicates that there is no way the Election Commission of India, or the voters will be able to distinguish between the real and a fake copy of the Electoral Rolls. This is a failure of the four protections listed here.

The use of unknown database to open 37 lakh bank accounts and transfer 167 crore LPG subsidies into them is another example. Another is the metering of broadband by ISPs to throttle speed or block content in violation of TRAI regulations and NET Neutrality.

 # What are obligations of parties who generate data while engaging in their common purposes?

It is necessary to develop a minimum set of binding obligations for transacting parties generating data so that this data can allow them,

or any neutral arbitrator in case of dispute, to be able protect the justice, equality, liberty and dignity of the participants in that system.

- Those who participate in the transactions of a system have an obligation to ensure sufficient data to protect justice, dignity, equality and liberty of all participants.

- Data may not be outsourced to data analysts to become entrepreneurs or build a digital economy off the data of the affairs of others.

- Parties, from within the transacting parties, responsible for keeping a repository of the data should document the agreed policies on creating the data, certifying it, authenticating its copy, restricting its use, auditing its creation, certification, restriction, updation as well as ensuring its fidelity and updating it.

- Any breach of data, at any time in its life-cycle, will be reported to all other parties of who have come together for common purposes. They should jointly assess and report the damages to their common purposes as a consequence of the breach to the law enforcement machinery for investigation and prosecution.

- Any disputes about data protection should be referred for arbitration under the Arbitration Act with machinery that can satisfy the requirement for interim relief within 48 hours in the matters of life and death.

I handed over a copy of this in the form of a letter to Justice Srikrishna.

Speaker: The adjudication mechanism is not working. It often leads to compensation and damages.
Justice Srikrishna: What kind of mechanism are you suggesting?
Speaker: Why don't we have an online dispute mechanism, where the judicidary inteferes at the end. The organisation or the regulator works this online dispute resolution. The redressal handling mechanism of digital india has failed.
Everything seems to be linked to consent. It's based on one single button which has I agree. There is no statutory mechanism which legalises I agree. It's dicey: how do we take it as evidence when I agree button is pressed. Is one sided contracts legal? **Lets legalise via the *I Agree* button where there is some statutory support.** Consent is going to be based on one button.

Deliberations have been going on related to a [Privacy law]since 2006. Aadhaar has been fining people when they keep data at a local level. You put an FIR on them, but what happens to that data? Huge amount of data is with them. Can't we have a right to purge? Courts will have better decision making power.

Justice Srikrishna: We are so focused on digital transactions, we forget what

is going on in digital life. That is required to be statutorily there for a specified period. Can we say that it should be immediately deleted or permanently deleted.

Speaker: What statutes are mandated, what is the amount of time that the data is withheld? Should be between 3-5 years, and other reasonable restriction in courts, till the matter is not settled.

Malavika Raghavan: Data risk is one instance that we're are interested in. The key question is, what is actually be personal data. Our proposition is that it should be personally identifiable information. We dont think there should be a distinction between sensitive personal data and personal data. We will end up landing up where we are now, with a meaningless list approach. The fact with big data is that proxies are used as links to information. The first proposition is that we should have one standard of personally identifiable information, and there is no excessive compliance issues there.

On NTPs: there needs to be a difference between controller and processor. If you can slice up the controllers into systemically important entities, medium risk entities and low risk entitied, and ex entities involve with them to prevent data breach. Pre-breach, what non threatening measures can we take. Can we give information guidance, and talk about private warnings, public statements ebfore you have the mass scale breaches before there is panic. On the point of consent, whether it should be a primary ground of processing: it should not be a primary ground. It should exist, but the role of consent has changed: it is a notice to the individual, and no longer is it a permission. All the obligations there should be a legitimate purpose test. There is a six clause formulation: whether the collection islegal, necessary and proportionate. So you balance the interest. Consent is no longer what you look to understand the right and the obligation, whether it is necessary or proportionate. If at any stage it fails the test, of collection, processing etc.

We've spoken with multiple providers who are seeing data as risk, and see it [data] as a toxic asset. Co-regulation is an important tool but it should be a part of the responsive framework. There can be a pyramid of sanctions, and a pyramid of support, for better data practices. One is the point of protecting individuals. Secondly it's important to enable data flow.

Rama Vedashree, DSCI: What is the framework that you have in mind to classify controllers as low risk, medium risk and systematically important?

Malavika Raghavan: The finance sector has some points: if you look at the Basil committee, one part of it is interconnectedness. A central database which a lot of databases use. Another is the volumes that they are exposed to. There are issues related to capitalisation. What is relevant is the amount of peoples information they are holding. When you categorise, organisations should have enhanced supervision tools. There are other tools that they could have. A lot of larger organisations are open to regulatory conversations. This can help reduce and minimise the risk.

Justice Srikrishna: Instead of being systemically important, it could be important from the point of view of the harm it could cause.

Malavika Raghavan: If you have at a market level the electoral rolls being called into question, that is different from inaccurate info for a few people.

Vikram Gopikar, TCS: My question is specific to article 2.3, which calls for retrospectice application, whether that would be feasible. There is an illustration in the South African regulation, within one year of collection, they need to be applicable to the act.

Justice Srikrishna: Data is already collected. All the data collected is capable of being misused. Should it or not be subject to the same stringency as what is collected today? Deal with it the same manner as it is today.

Nancy Jane: There are laws missing: for example IT guidelines for cybercafe rules. Quite often we give this information, and the data is both digital and non digital as well. Both the non digital data should be protected. DSCI had come with a manual. When the police collects data, in case the data is leaked it affects the image of the victim. There are times where rape victim videos have been leaked. Related to corporate espionage, should juristic persons be protected? they should be. Considering that there are lot of infringement, we should protect their interest as well. There is a responsibility to protect that as well. Data protection should be retrospectively applicable. There should be a time-frame given for compliance.

Aditya Birla group representative: A lot of data is going to be with the government and it should be the role model, and Aadhaar data is with the government. There are chances of leakage. It's important that we apply the principles as well. Another important point which the industry is facing is the extraterritorial jurisdiction. If we could have a treaty at a country level for a safe harbour, it would help us.

Justice Srikrishna: What are you suggesting when you're talking about extraterritorial jurisdiction? Is it data pertaining to India, or to Indian citizens?

Aditya Birla Group: If it's an Indian citizen, there should make the person accountable if they're extracting the data. Thereby the citizen of India is feeling secure. From a GDPR perspective, the way the law is, that they have extraterritorial jurisdiction. Somewhere a treaty as a global level.

Justice Srikrishna: That is a matter of international treaties, and not of the law.
Aditya Birla Group representative: I don't agree with the principle of localisation of data, but certain sensitive data can be localised.

Ashwin, VC: Related to anonymised data: it's practically impossible to use anonymized data, and ensure that it cannot be used beyond the scope. Anonymised data should be defined which should be out of the purview of private data. That is needed because many laws and frameworks cannot be

implemented on certain data, in terms of scope. It's practically impossible to define the use and inform the user.

Krishna: We should stress on privacy and data protection of India, instead of data protection act. We need to stress on it, and keep on repeating privacy, privacy privacy. We need to consider social cultural aspects of India, we have specific sensitive elements. When we define the personal information and sensitive personal information we need to look at social aspects. Consent is coming ahead of notice in the draft, ahead of consent. Notice needs to be ahead of consent.

Anveshan Roy: We work in understanding movement of people in and out of locations using wifi analytics. Our recommendation of MAC ID should be non personal. Every device has a MAC ID, and that is not personal information. Seeing the potential in India. One cannot identify the person by the MAC ID.
J Srikrishna: How is it not personal?
Anveshan Roy: If you have a wifi router and a sensor, your phone has MAC ID should not be personal if it is anonymised completely.
Gulshan Rai: Technically it is possible to identify the MAC address of the person.
Anveshan Roy: If I'm the only personal in this room, I can do the reverse engineering. MAC ID has to be tagged with other form of data capture. For us, the initial bit is anonymised and aggregated. We're not capturing IP address.
Anveshan Roy's Colleague: MAC ID is not identified. If it is merged with another data sourced, consent should be required.

Another speaker: IP Address should be under the personally identified information. Each category in sensitive personal information should be very very well defined. Regarding the children, in cybercrime, most cases are children related. The pictures should be asked only if necessary. People take pictures, upload it. If it's a 16-17 year old, the pictures are going into the dark web. We need to take care. Take it only when necessary. They should give them an option, even when the school is storing this information in its database, we need protection of data and enforce certain rules. The concern is of privacy of children. The last point is: even parents, are posting pictures of children. Some warning systems for information like that.

Malavika Raghavan: On the horizontal application point, it would be meaningless to have different laws. The interesting one is around jurisdiction: one is the territorial jurisdiction, it should be everyone in the country. no provider can check your citizenship. There are companies who are conducting business in India, anyone buying goods and services should be protected irrespective of where it is being delivered from. Where there is an entity outside of india, and there's a process, even there, where that processor is processing data in India, there should be a cause of action against them.

Identifiability and anonymisation: it must be a technology neutral law. The questions will be specific: the first is related to the identifiability of the individ-

ual. The law applies to an identifiable natural person, and this can be defined. You can provide a list which is indiciative list at a principles level. Anonymation and pseudonimisation technologies are evolving, if its not identifiable then its not applicable. We can come at clear articulation.

Justice Srikrishna: if it's not applicable today and is possible later, the law should apply later.

Gulshan Rai: How do you classify rights on entities outside of India?

Malavika Raghavan: The first is the jurisdiction clause: Foreign companies doing business in India, second is whether they are data controller or processor for our purposes. The offering of goods and services, you would have a claim under the consumer protection law. Purely on the fact that they're offering goods and services. There is a legitimate purpose test….

Gulshan Rai: He's a data collector when you open the account. The other is when they are storing the data.

Malavika Raghavan: the third aspect is legitimate purpose. We will need sector specific regulations.

Anupam Saraph: A concern: increasingly there is a trend that harvesting of information is normal and natural. It assumes that there is nothing wrong about it. If we have to protect somebody, and protecting people who are transacting parties The minute we forget that, where I can photograph and bug you throughout the data, or access to your bank account that I have the right to harvest for whatever purpose, is completely irrelevant. There is no wilful consent and participation. There is no legitimate reason for collecting this. I think this as a big concern. Who are we protecting and whom are we protecting them from. If we don't define these two parties, then we would have lost an opportunity to say that data isn't the new oil. it's not another commodity, It's about ensuring that by protecting data we can build transactions of parties within the country.

Justice Srikrishna: That's where malavika's formulation about consent. There is accident and evidence. The purposiveness of the test becomes important. The purpose for which security camera will get a tick mark.

A speaker: The lessons from the IT Act have to be implemented. The implementation lacks the teeth. The second is the awareness to the data subjects. Are we making some efforts to tell them what is privacy.

ICICI Bank representative: On purpose specification and a citizens choice…One citizen might not want to get offers given to them which is not directly related to what they have given consent to. There would be others who would want this information. A choice to the citizens should still be kept, and citizens should be given an option to opt. There's massive criticism on clickwraps, unless people agree to the terms and conditions. If we want to give someone an option, should the law prescribe what should be informed consent?

The person may not choose to get the information, but the service should still be available.

Notices which are to be given, the paper talks about consent fatigue. From an industry perspective there could be a common notice, which could be framed with the sectoral regulator. Every bank is going to send a similar notice.

Often there is a requirement to source customers. Once a customer comes and engages with an organisation, it is only then they enter into a contract. When you are trying to source customers, like in club diaries and industry manuals. How should that organisation be liable for using that data which is in the public domain?

Justice Srikrishna: If I become a member of the club. I give them my data. I give for the purpose for my association with the club can be carried forward. If you as ICICI go and take it, isn't it a failure of the purpose test? I didn't allow the club to give it to ICICI or HDFC? How you source your data, you find out what can be done. But today I get emails from ICICI.

ICICI Bank: There's a distinction between sensitive personal information and personal information. How we were perceiving that was in terms of the harm which is caused. In the prospective list, under the SPDI rules, it includes financial information. While all other constituents, which is intrinsic to a human body, the harm which can be caused with that data is different from financial data.

Justice Srikrishna: Financial data is personal data. Tomorrow someone finds out you have Rs 100 crores in the bank and you'll get a call from Dubai. Sensitiveness to data is apart from the inherent nature of the data. It is sensitive.

Gulshan Rai: Malavika was saying that you raise the standard of personal data [to sensitive personal data, and not that you reduce the standard of sensitive personal data to personal data].

Professor Nagarjuna from TIFR: The law should have a directional principle, where you would say what kind of measures would enhance data security. There is a linkage of information to a large number of agencies. One clear law that one can make is to say that the greater the linkage, the greater will be the leakage. If you have 1 billion people, each person has at least 10 social service leakages, there will be 10 billion leakages. Therefore, is it int he scope of this document to specify what kind of measures would enhance data security? Could it say that linkages to various services should be reduced. There may be business interests, and other interests, but not in the interest of citizens. Greater the harvesting rights given to people, the security will come down. What are the models that will decrease or increase the data security. We are talking about data processing techniques. We need a public audit of data processing. Similar is the case of encryption, rather than some expert committee, because there is a possibility of selection of experts. It's also important for us to say that when I give consent, the agency should also give an undertaking. There are devices that

we use which have device identities. They are potentially capable of becoming sources of harvesting.

Justice Srikrishna: You're saying that there should be an undertaking. Why is it needed if the law says you're liable. Undertaking is what he tells you as private contract.

Prof Nagarjuna, TIFR: Doctors give an oath. Those are some kinds of roles and responsibilities.

Justice Srikrishna: (something on the lines of an oath is a moral commitment, and not enforceable).

Sandeep Arora, Market Research industry: One of the things that I've noticed, is that we seem to be too worried. We're seeing the dark side. In this world today that there is so much data that it can help people. We're able to understand the causes of diseases. We have the technology today, it would be foolish and myopic that we don't do it for the better benefit of the humankind. I would want to enhance the motivation of the law, that it has the necessary balance in place for us to ensure that the benefits that it brings to people and consumers is kept in mind. I have a couple of points: In market research industry, we need to keep understanding people. It can lead to a state called mass customisation. You can give a larger solution at an aggregator level, we can understand mass customised solution raise. We need to keep understanding a person more and more. If you have understood them once, you can go and ask questions all over again, or you can go to a proxy and start from thereafter. For us it is very important that we are able to maintain and get incremental insights.

On the quality checks: we have to go back and perform the necessary checks, and for that we have to maintain recontactability.

On informed consent: There are two-three elements. One is a blanket consent. Do I really, as a consumer, a right to negotiate different parts of what I'm consenting to. I have to go and agree. There are some dark elements sitting there…

Justice Srikrishna: When I go for a LIC they ask me hundred questions, and say I give you only my name and age? Therefore, the larger test would be purposive.

Sandeep Arora: Sometimes we are not able to understand the purpose.

Ranjeet Rane from Reserve Bank IT, speaking in personal capacity: I think that the law should take into consideration that in a very small span of time, we have sene concepts like password become irrelevant with technology. For example, fingerprints. On the financial information side, the law should list down what should list down what should be sensitive. Considering that we are aggressively pushing financial information, I would request the committee to have a view to look at financial information as sensitive personal information.

Beni Chugh, Dvara Research: Two issues keep recurring: for how long should the information be retained. If we think of legitimate processing test as a step

of the framework. It's more of a framework that we're proposing. The CICs are required to retain data for seven years. For other records like vaccination, these are taken care of by the legitimate processing test. There is a need for sectoral regulators to come. On consent, there is behavioral eocnomics to show that it cannot be the exclusionary ground. On one hand, you have legitimate processing, and the obligation to not cause harm. We come at a solution that emerges organically. If I take a photo at a photo booth, it cant be sold on the dark web.

Shagupta USIS: In terms of the right to be forgotten, it does not allude to the context. To our mind the use should be very limited, in case of theft and financial fraud. It would be better to have broad principles. We saw TRAI and CCI getting into a conflict. The third part is data localiation: that there shouldn't be blanket localisation.

In terms of data processors and controllers, there are intermediaries. They might not be processing or controlling the data.

(made some more points but spoke too fast)

Data minimisation should be replaced with a no harm principle, with artificial intelligence coming in.

The penalties should be in proportion to the harm. Just because the companies have high turnover….

Wrt children, we feel that there could be 3 categories, where it is less than 13 years, where parental guidance is mandatory. Next is 13-18 with individual consent along with parental guidance, and then above 18.

Vickram Krishna: Much of what is concerned with communications impinges on the pesonal sphere. We are close to a cusp where we are in a position to be a serious global player again, provided we have the right laws. One thing that is criticial data management. If there is some place in the world where it is very very important for how personal data is handled, that is a model that we have to respect. If you look at Germany, one of their largest auto makers, Volkswagon cut a sorry figure where they were trying to defeat global standards. What's worse is that Germany has taken a hit for the understanding of technology. We should be setting an example to the world for how we can respect the personal data of our citizens at a level that is at least as high. This is really an opportunity for us and we must take it.

Suvendra Tulsian: It looks like everyone is overcautious about data. Law should be practical, but we cannot ignore the technology. Law which is good for Europe is not necessarily good for India. Most of the discussion is about protecting data at storage or in transition. Look at the way data is generated: Whatever data we have with UIDAI is protected. Can the UIDAI guarantee that the fingerprint they're getting is not getting leaked? If the whole purpose of UIDAI is properly authenticating the user, they cannot guarantee authentication, how can they allow financial transaction using Aadhaar. One is the consuming party and

other is verifying party. The law should make both parties liable for ensuring that the right fingerprint is submitted. The third suggestion is about MAC ID, that one should be able to capture it. In IOS and Android MAC ID is not allowed, because they understand that this is a problem. Because directly and indirectly one can reach the person. We need to recognise the machine but it should be using a virtual ID, not MAC ID. The only use is on the organisational side. What the device is the company shouldn't come to know.

Harsha Vohra, Data Locus: In the previous law there were definitions of data and access which were broad. We had to take legal opinions from multiple law firms, and not even two of the opinions were same. At the same time, companies in western countries they could formalise a code of conduct. My request is to a data protection authority which could be used by entrepreneurs to take a decision before they start up. We've seen that a lot of innovation is not happening because the laws are not clear. Companies in the US which work on images captured by satellites. Laws can be formed to help in these kind of innovations.

Shreyas Bhargave, Capgemini (personal capacity): The need for physical documents as proof when we're doing eKYC. If we talk about data security on the digital and physical side. Can the law specify remove the need for physical documents if we're doing in a digital manner.

Justice Srikrishna: People collect for purpose. Data minimisation is the principle.

Speaker: gives example of new android guidelines, and says that there should be function driven purpose limitation.

Justrice Srikrishna: That is what Malavika (Raghavan) was talking about with purpose driven regulation

(Someone sitting in front of me turns around and says to Malavika: This will be called Malavika's Data Protection Act :))

NS Napinay: I was under the impression that the consultation was going through follow through in the question format. I have a lot more questions than answers. We are faced with a situation where dolls and toys are collecting data, TV shows are facial data, not just usage behaviour. Whether it is offline or online, we don have ring fences protecting information. India has the advantage of doing cherrypicking. The white paper has a west to east flow, in terms of laws. We are on one hand are looking at taking from robust regimes who have learnt from their mistakes, and we are looking at jumping on the bandwagon and going to the gdpr. How ready are we? How much confidence can we have of data controller with just conformance rather than compliance. We've had some skeleton laws in the part of the IT Act. They prescribe certain provisions. Every single provision has been treated more as a tick mark. We may even have a due diligence. Each just leads to a report being filed and it doesn't reflect reality. 90% of what is laid down will result in compliance, but even in the compliance,

if we can ensure that merely the tick marks protects the individual rights, we would gain.

Justice Srikrishna: Vishakha guidelines have been in operation for so many years. Every company has to have to have a special committee to deal with sexual harassment. What implementation do you see on the shop floor? The law is good. The mindset has to change? Is there any solution?

NS Napinay: only two things drive the world: Fear or greed.

Justice Srikrishna: that is right, so we have fines on global turnover, or prison.

NS Napinay: the command and control and coregulation: Self regulation and coregulation have always worked better than command and control. Command and control only works only if we have a fear of retribution which results in its adherence. That's the way we might have to go with data protection: not just the kinds of data, but also balance thekinds of protections we are putting for each kinds of data. What is the purpose: to protect the individual, empower, enable them or just to enable governance? Is to enable businesses, whether big data analytics. One flip side of this is that businesses need as much leeway with data as they need a law. If we don't have as much of a robust law as the EU GDPR, so business comes here. It needs to enable rights and puts the individual at the centre. The governments rights have to be balanced based on the social contract theory that it is the individual that prevails. "And the law hangs limb, and barks but never bites". TDSAT cannot be an authority to decide on data protection, or cyber issues. The secretary ministry IT cannot be the adjudicating officer. When I look at the Schrems case, my utopian dream would be like the EU Court of Justice in India. If that isn't enabled, what will the act be about.

[Came in post lunch]

Rahul from HUL: Part of the data governance team, but speaking in personal capacity. For most of the ecommerce companies now coming, the natural method of the business means that they collect a lot of data. One big purpose is enhanced consumer experience. The other essential entity is the manufacturer, whose product is traveling back to the household. Manufacturer also wants to enhance the consumer experience. If there could be a check-button which allows the consumer to say that I want to give the data to the manufacturer.

There are many companies in the space of technology who are servicing consumers and businesses, and there's always a chance of interlinking data from one to the other, which gives them a magnitude of strength. There are entities like Google, which has its android platform which can be shared for their services too.

Debashish Bhattarya from Broadband India Forum: There has been a lot of talk about why we need to protect data. Just to play the devils advocate, where data has not been use to harm anyone, to write the law in a manner that kills sources of innovation is not a good idea.

Today India is being looked at a global knowledge hub. We are undergoing innovation which is data driven. Data innovation and privacy can be compatible. The data driven innovation cannot be scaled without adequate privacy safeguards, without the trust of the users. Hence it is critical to empower users without overregulating. The law needs to be outcome driven rather than prescriptive.

Secondly, collection and processing of data should be allowed with minimal restrictions, where there should be control for the data subject, with the right to recall and opt out, and the accountability for the data controller. The next point is that preventing harm principle is a better approach. In terms of the comparison between the roles for the data controller and data processor. The law should not unreasonably intervene int he relationships between data controller and data processor.

In terms of a data protection authority, there should be corporate accountability and an ombudsman, the principle should be a self regulatory model. Only in case of a deviation, the ombudsman should have a right to intervene.

In terms of right to be forgotten, it should be for information not publicly available information.

IIT Mumbai professor: Oil produces production and should be taxed, and therefore when you're using someones data, they need to give proof and why they're using it for. The onus on collecting the data is on the controller. There are now tools available, and philosophies like distributed computing, privacy by design. Things are possible. Why not have laws that are not enforceable? You could make references to these things to give direction. Data has two roles, like a knife: for murder or cutting vegetables. We are formulating new laws. Google and Facebook are very powerful. These are very powerful entities. If it fine to have a legal framework in which they manipulate and control us.

Ajit: On data localisation, I have a view that asking for data to be localised put a lot of problems from an economic perspective, but is there way to force service providers to give direct access on an MLATs process? If that can change then that is reasonable. Something which says that anyone who provides servies in the countries, that woul dbe good. We shouldn't be asking for data localisation. I don't see anything in the paper about information on dependent entities. What are the expectations from a privacy perspective?

Cognizant representative: We have captured things from a transactions perspective, and most clients say that India isn't adequate. They offload a lot of things on us in the clauses and tehre is no negotiation. The business team has to think about an Indian version of GDPR, with the same rigour. If the committee could take that into view, while drafting a bill. In terms of access to data by data subjects, when requested by data subjects, we need to give access and modify.

In terms of the DPO, it is a cost. If the law imposes such a requirement, it is a cost. Our submission is that please keep that flexible to not keep an in-house

DPO and outsource to an agency like a company secretary.

Puneet Awasthi, Market Research Industry: We collect personald ata and opinions. If a person after a year of volunteering that information, and if a large number of people do that, then that has a huge impact. RTBF should be for personal identifiable data, and the analysis should remain. There's also under element, around defining elements that constitute private and personal data. There are data which are not identifiable with a biological entity.

Shivani Nadkarni: The law that comes out will create an ecosystem of auditors, DPOs etc, and one the biggest challenges is that the awareness is very very low. Very few people understand the difference between data privacy, data security and data protection. The awareness levels need to be increased. Some suggestions I had: There is a mention of bringing out a pictoral notice. What are the other ways in which consumers are in a position to understand and take a decision. Organisations could be helped with specific standards and guidelines in ther form of seals and certification, which helps them understand the level of risk and compliance and thus take a decision. The law could build in structures to build these kind of implementation.

Ayushi Mishra: Is this law on the horizontal level or the vertical level?

Justice Srikrishna (with a twinkle in his eye): The law will be spherical in nature. It will cover all 360 degrees.

Naman from Access Now: [gives too long an intro about Access Now] There needs to be the withdrawal of consent, allowing the data to be deleted. The second would be regarding self regulatory mechanisms: in euripe and otherwise, only mandatory frameworks work and are required. Industry inputs in terms of what they should be and how they should evolve, and are required.

Brinda Mazumdar: The scope we're talkig about in terms of natural persons, looking at both the living and the dead. Even dead persons personal information could be misused.

Justice Srikrishna: In Puttaswamy, no one argued for a dead persons aadhaar number.

Ayush, from Bloomberg Qiunt, speaking in his personal capacity: There has been a mention about informed consent. The point I want to make it is that people have concerns around the data that the big tech companies have. The first is that the monster in terms of what access they have, is a lot more nuanced. The kind of permissions that we're giving these apps. In the UK everyone talks about iOS giving more secure than android, while Google is facing a class action suit, where data was accessed by Google. Google's response is that they used a Safari workaround. The case has only come up now. The second one is that Uber has been in the news for all the wrong reasons, where Uber was accessing location even after completing the trip. I don't think it's black and white.

My concern is that when you speak to them, they dismiss it on a technolog-

ical ground, else they say please fight this out in California. These big tech companies shoudl we have a robust enough framework to bring them to court.

Justice Srikrishna: whoever operates in India is subject to Indian law.

NSDL representative: With regards to consent, there should be a lifecycle of the consent, and they ought to take a periodic consent. Many times consent is drafted, the individual is not allowed to say no. For example, if I'm giving KYC data to a bank account, I could be asked to give the data to the credit card. In terms of revokation of content, I shoul dbe allowed to revoke consent. In terms of data collection, does the consent also apply to other information that I have not submitted, which they have to acquire from the third party.

In case someone dies there should be an heir to the data. The heir should have a legal authority to take authority to take action. So many times, the data of the dead can be misused again the living. Protection of the livign because of the data of the dead is also important here.

What happens if I collect data from the Internet, why can't I use the data? how can you say its misuse of data?

Medical data and financial data is contradicting: if I'm in a coma and someone needs my medical records, will my consent be required?

USIBC representative: supports a light touch regulation with freedom of movement of data. It recommends that the govt prepares privacy principles similar to OECD.

***

Nikhil (that's me): made a point about mass surveillance and why governments need to be governed by this law, and there were judicial oversight mechanisms which were not allowed as amendments to the Aadhaar act; the need for data minimisation, poor implementation of Aadhaar which is putting citizens at mass risk; also the problems with mass customization and predatory behaviour; the need for consent because consent is a switch (countering Malavika Raghavan's previous statement about consent primarily serving the purpose of notice.

Another Speaker: Sector regulators have sometimes been bought in. It would be a problem if we allow sectoral regulators to determine granular parts of the law. We ould end up areas where the same individual and same data is seen under two microscopes. The last point is of due sunset clauses. Will we do it for one year, five years. Having such a clause would help such a law be futuristic, where we can go back to this law every three years.

Justice Srikrishna: You're talking about a suset clause for the law?

Speaker: There could be clauses that would need to be checked for relevance periodically.

Suchana, Hindustan Unilever: On the point on consent around medical issues, as a corporation we often are at crossroads where we have to decide how much

to share when one of our people needs medical information. Thus, taking informed consent when I am the custodian. The law can provide exceptions for reasonableness considering exigencies, and security measures that I need to take before sharing.

Justice Srikrishna: the whole idea is for everybody to understand what everyone is saying

Malavika Raghavan: I wanted to provide a couple of ways in which we could look at the liability section. There's a section on accountability and enforcement tools. If we look at the objectives to promote the agency of people,

Justice Srikirishna: benefit and empower, give them control and prevent harms

Malavika Raghavan: The formulation that we're thinking through are a list of rights, which will be the fount of the obligations. You must take consent, you must allow access to data, there should be a statutory … you could allow strict liability standards for specific rights. The good thing about strict liability, if you're thinking about insurance, it always need a strict standard. For the ex ante measures, you should have strict liability. The second level is this idea of harms, and there are regulators who have started defining harms: They've worded it widely in terms of actual injury or loss. You can have a reasonable efforts standard for this. We should have a reasonable clear standard for the right to informational privacy. The interesting thing is that we are not actively misusing data. The IT Act does so. None of this is that we are new to. In India, nothing will work because we don't have regulatory capacity.

Justice Srikrishna: We are concerned with normative standards.

Malavika Raghavan: Firstly when we think about the powers of the regulators, we want to make the case for ex ante supervision before the breach. Every time we've had intersectoral coordination in case of ULIP. The FLRC recommendations did look at private and public warnings. You could have a range of investigative powers. It is useful for the regulators to escalate some of these things. IF you have a regulator that speaks softly but carries a big stick is in the insterest of the ecosystem. Two other things: a complaints database. The consumer regulators in the US. Aadhaar already has a complaints databse. You could look technology to mine this data and have a heatmap for which types of agencies. The other is the notion of reg-tech.

Justice Srikrishna: There could also be a complaint about the privacy of the organisation where it could be used to victimise.

Malavika Raghavan: It could use differential privacy and a frequency graph. The other issue s the accountaiblity of the regulator. It could be the enforcement directorate. That transparency is important to signal the market. Ex Ante these things need to be looked at.

All types of national identifiers, there need to be some restrictions around their disclosure and use. These should be use limited. There was a final point around

data controllers. Because we talked abou tentities interating with consumers who are not the controller. Any entity interfacting witht he consumer collecting the data. the reason why this is important: they only perform an aggregation.

Justice Srikrishna: There is one entity which collects data, does not process, hands to A, B, C, and if there's a breach at the end point who should be held liable?
Malavika Raghavan: Data controller is the person who is collecting data from the user. And the person for whom the data is collected. Everyone is a processor or a controller, and there should be joint liability.

Rajat Moona: In IPC the notion of accomplices is already there.
Vickram Krishna: We've seen in India, that the amount of concentration of corporate power is following the same pattern as conglomeration in Europe. The second is that we all take it for granted that Antarctica is meling. We have arguments about why it is melting. But people are convinced taht it is because of human action. So we don't take it for granted. What I found missing in the white paper is the possibilty that w ehave some other way of managing our production, our productivity. We dont think of civil society as being productive. That's not the way it used to be. There's no recognition of it in the white paper.

This is the new production.

Speaker: There is one way in which it leads to data protection. Any centralisation leads to data vulnerability. What are the ways in which citizens can be empowered is a distributed model. Empowerment of citizens. What is the time when data protection would enhance.

Justice Srikirishna: lets forget the law totally. Today someone will ask you your name etc etc. Person might do it because they want to give you better service.

Speaker: Instead of a single large silo.

Srikrishna: Data collection is a fact of life. There should be a right for people to say dont do it, dont do it for this purpose, use it for this purpose.

Speaker: We can set the direction in which it is moving. I want to keep my wallet in my hand.

Other speaker: About the exemptions proposed in the white paper. There should be certain minimum obligations. For example if you have for personal use in household purposes, for example matrimonial lists whic can be published online. You could have an app like truecaller. Soe obligations nad restrictions need to be kept.

On national security, you have the DNA data bank, for investigative purposes, but ithas huge potential for violation of privacy.

Srikrishna: it's to do this more scientifically. The DNA data bank. It should be done or not be done?
Speaker: The first draft suggested collected the data of everyone.

Srikrishna: The criminals are limited scenes of crimes, for the purpose of modus operandi.
Speaker: The second draft removed that and restricted it to criminals. The data protection authority should have the power to prevent it. Then there are searches of devices at the borders.

Update: Asheeta Regidi, a technology policy lawyer says that these were her points, and clarifies further:

> "My point was on the exemptions- that they shouldn't be drafted too broadly, and minimum obligations and restrictions must be in place. One example is the exemption of personal use/ household purposes- where you can have a matrimonial list created for circulation among private members of a society (a personal use), and is then published online via a blogpost (a privacy violation). Similarly, address books could be exempted as a personal use, but you have an app like Truecaller which collects it into a publicly accessible database.
>
> A second exemption is that of investigative purposes/ national security. These should not be drafted in a way that prevents the Data Protection Authority from acting against a state violation of privacy. An example is that of the proposed DNA databank that is to be created for investigative purposes, but has huge potential for privacy violations (looking at the first version of the draft bill).
>
> Another example is the border searches of devices as seen in the US, which could be exempted in the name of national security. It is important that privacy obligations such as collection limitation, storage limitation, data erasure, etc. (and not just purpose limitation, as specified by Justice Sri Krishna) apply to the data collected at such points. The DPA must retain the authority to act against such violations."

Another speaker: DNA and fingerprints are collected by police authorities. At times govt has an exemption. But the liability for them is much lesser than for the normal people at large. The standard of liaiblty should be the same.

Manoj: Like investor protection fund, we can have a consent protection fund. It will reimburse users in case of breaches as a compensatory measure. So that unnecessary prohibition of data. Secondly, self regulation.

Rahul Sharma: On the aspect of building in privacy by design. Singapore has it in its national cyber security strategy. Should it be law or a part of standards. There are roles for sectoral regulation, etc etc, and then try and figure out what everyone will do. Usually laws do not have a sunshine period. We should have this.

GDPR is increasing the cost of compliance, without enhancing security and privacy. There has to be a proportionate increase of security. The cost gets transferred to users. Data localisation was a protectionist strategy. We have an

opportunity to counter this. The government can ensure it for its data, but not for the private sector.

Nikhil from UTV: While we support notice and consent, the restriction that consumer facing industries that are not able to take consent, but consumers are willing to get it. Two year timeline for implementation of the law. It'll take

Suresh Menon: At Maharashtra government, we're setting up blockchain. Currently I can only way I can improve it improve my SLAs. We should come out with guidelines of distributed computing, for deleting.

Anupam Saraph: I want to thank you for actually saying that you'll be technology agnostic. I'd like tyou to be agnostic to words that we import fro m technology. One is the idea of ekyc. ekyc and kyc are two different things. ekyc can be used in N number ofplaces, and there is no way this can be prevented. This boils down to import of concept from technolog. The second is the idea of identification. There is no idea of identification in authentication. To use authentication where identification is required. I'm going to stop here because this is important when we are going to talk about data protection pertaining to the digital space. In digital, all of these concepts, you don't think about how you have changed the responsibiltiy of the partners who have been transacting manually, and sometimes you end up throwing out the responsibility from anyone. It's important that we understand the business process. It has nothing to do with technology. By digitialisation they should not be able to throw out responsible parties from the process. Branch manager used to be responsible for opening an account. With Ekyc, no one is responsible.

*

(Note: In case you spoke at this event and you want to share additional points or share corrections, please feel free to mail me at nikhil@medianama.com. We'd be happy to append additional points or clarifications with the original text above. If you took notes and published them somewhere, please share with us, and we'd be happy to link out to them)