#NAMA: Impact of Personal Data Protection Bill, 2019, on companies

The Personal Data Protection Bill, 2019, was introduced in Parliament in December 2019, and was referred to a 30-member Joint Parliamentary Committee for review. The Bill is the first legislation that focusses on privacy of citizens, and could potentially result in significant overhaul of digital businesses and companies. The Committee is expected to submit its report to the Parliament before the Budget Session concludes on April 3, 2020.

Earlier this month, MediaNama held discussions in Delhi and Bangalore on the main aspects and impact of the Bill with a wide set of stakeholders. The discussions were held with support from Facebook, Google, and STAR India in Delhi, and with support Facebook and Google in Bangalore. The discussions were held under Chatham House Rule, so quotes have not been attributed. Quotes are not verbatim and have been edited for clarity and brevity. Read our full coverage of the discussions here: #NAMA India's Data Protection Law – January 2020.

The following is Part I of our notes from the session on user rights and data fiduciaries,read Part II here.

What will be the impact of the Bill on companies? How difficult will compliance be?

Being India's first comprehensive data protection legislation, the Bill is going to have a fundamental impact, said a speaker. "The current law, the IT Act, places limited obligations on companies, and only regulates sensitive personal information. With the new law, companies will have to overhaul operations, reconsider business practices, think through their plans, strategies, and the way they are using data," the speaker noted.

Compliance would have to be done in three categories, another speaker explained:

- Basic housekeeping, such as whether companies have the right security practices, purpose limitation, storage limitation, etc.
- Securing user rights such as data portability, right to erasure, etc.
- Compliance by significant data fiduciaries, including preparing impact assessment reports, which will be a disproportionate burden on the significant data fiduciary, and which the Data Protection Authority (DPA) will play a role in.

On the role of the DPA, the speaker pointed out that the regulator "has to make decisions on at least 40 and probably significantly more aspects of the Bill,

ranging from user requests, whether companies can charge a free, anonymisation standards, etc. These rules will affect start-ups and determine compliance cost. The challenge will be how to ensure that the rules are framed in a transparent, consultative manner".

What kind of compliance time frame can companies expect?

Depends on size, activity, scale, etc.: Since the bill will come into effect in phases, different activities will be affected at different stages. The duration companies will need for compliance depends on the scale of their operations, how complicated their data flows are, how much data they are collecting, how many different countries they are operating in, how much sensitive personal data they are dealing with, etc.

Some businesses have said that six months is all they need. "Companies who are already compliant with GDPR, may be already compliant with the Bill to a large extent, although not in some critical aspects."

'Data is the new oil': "The nature of our Bill is fundamentally different, since our Bill is only in part a Data Protection Bill, it's also a 'data is oil' bill, which makes it a little more difficult to comply with."

Depends on DPA: "A lot also depends on the DPA's regulations and its classification of companies as significant data fiduciaries. It's unclear what companies can substantively do about it right now."

Not much that companies can do until regulations come: "Companies can start thinking about and considering the Bill, but they can't do much until the delegated legislation under it emerges. The Bill is strictly principle-based and companies don't exactly know how to begin compliance. The practice-related aspects on how to locate data in certain jurisdictions, the compliance processes for data collecting, processing, storing, etc, how verifications would be operationalised will only become clear later."

But companies *can* apply the best-in-industry practices to hedge their bets. "A good step would be if the industry playing an active role once the DPA, and be active in figuring out the regulations, practices, and standards it will set. For instance, a regulation on encryption or anonymisation should ideally say 'do best available', or do 'best-in-industry standards' as opposed to prescriptive directives from the DPA."

Industry associations will have to be proactive, and bring in codes that work for companies. Since the DPA members also aren't needed to be experts in data protection, it would be a good idea for industry to get together and decide best practices."

Dealing with privacy-by-design policy certification

The definition of the privacy-by-design policy in the Bill is quite open-ended as it talks about operational and managerial policies, as well as technical standards, pointed out a speaker. "Organisations will have to develop privacy programs, and then they can ask the DPA to certify each and every organisation's privacy programme. This will be extremely cumbersome for the DPA," the speaker said. Under the Bill, every data fiduciary has to have a privacy-by-design policy, but not everyone has to submit it to the Authority, noted another speaker.

Although such certification exists under GDPR as well, "it's voluntary and organisations choose to get their certifications because it looks good for them". Moreover, the burden for certification "is on outside certifying agencies, and not the regulator," the first speaker added.

How the policy has to be formed, and the time frame for submission, will be determined by the DPA's regulations. "**Even with this, there's too much discretion with the DPA. It could say that everyone has to submit the policies or may it could ask only select fiduciaries to submit it. Again, there's no transparency around how it will arrive at that decision,"** pointed out a participant.

How is it different from the 'Data Trust Score'? Under the Bill, an auditor will give an organisation a 'data trust score', and the data fiduciary is supposed to put it in their privacy policies. The same requirement exists for the certifying privacy-by-design policy. The only apparent difference between them is that data audits will be conducted annually, but the privacy-by-design-policy certification will happen if companies make changes in their privacy program over the course of their certification period.

Regulating social media intermediaries: why?

Why are they in a 'data protection' bill? "The inclusion of "social media intermediary" has come out of nowhere," a speaker said. The government has been trying to regulate social media entities for a while, and it has been inserting regulatory provisions for those companies in whatever legislation it can, the speaker continued. Another speaker asked if it has anything to do with data protection: "This comes from the issue of traceability in the courts. It seems to be something that is being done under the guise of data protection," the speaker said.

The verification requirement in ironic: Although a data protection act is meant to ensure that organisations don't have more personal data than required, the verification requirement unnecessarily ensures that social media companies will have access to sensitive personal data, the speaker highlighted. "You're just giving them an additional, very crucial data point to actually have more accurate profiling and surveillance, which doesn't fall into the objectives," the

person said. According to another speaker, "an easier and smarter solution would be to allow verification of messages rather than people."

And it's difficult to implement: According to a lawyer, the verification requirement will be challenging with regard to children, since the Bill requires that their age be verified, and parental or guardian consent needs to be taken. "The child user may claim to be a certain age, but there is no way to make sure that's that is actually their age," they explained.

It also compounds the regulatory problem: "In India, regulators suffer from the problem that their mandate is not clearly defined," pointed out a speaker, adding that "until 2016, it was never specified what is the RBI's job is."

> "Similarly, the DPA's job is data protection, but the government is trying to bring in countering misinformation into the same Bill. In the process, you end up creating an authority or regulator whose mandate is not clear and so they have a lot more discretion than they otherwise would," a speaker said.
>
> Additionally, since the DPA isn't independent, "it essentially creates a very unaccountable structure, which allows the government to do a whole bunch of different things without necessarily sticking to the mandate of this bill."

What's a consent manager? What could it look like? How does the Bill regulate it?

The closest parallel to a consent manager would be the NBFC Account Aggregator framework, said a lawyer. The idea germinated in the Justice Srikrishna Committee report's idea of a 'consent dashboard', noted a speaker. Under the Bill, consent managers will be a new category of entities, and they will be data fiduciaries, and will be in control of an individual's personal information, will be able to make decisions about that information, said a speaker. Other speakers had several other guesses about what a consent manager could be and do:

- The consent manager would be a third-party service that allows a user to bring all their applications on the same service, and define which application has access to which category of data for which purpose, for how long, what are the retention periods, how can it be stored, etc. The user may be able to manage their rights under the Bill — some of which are rights to confirmation, access, erasure — via the consent manager.
- The consent manager could be like a wealth manger, that is, a trusted expert to manage user consent. Or it could go the Account Aggregator route, which would make it a one-stop shop to view all your permissions in one place, make it easier for different business to go to one entity and get access, pull whatever information the user wants from that one entity as opposed to going and talking to 35 different entities, and so on.

- The reason it's a data fiduciary is because it will have user's personal data, such as the email address, and which platforms it's associated with, perhaps the user's age, phone number, etc. Therefore, it becomes a data fiduciary since it independently also has access to user information, and also has access to the user's information from other platforms.

One of the speakers, who is also a lawyer, said consent managers look "wonderful on paper", and even the Srikrishna Committee said they were a good idea, based on the Account Aggregators framework. The Committee had observed that:

- One method for managing consent is to ensure that every data fiduciary has their own consent dashboard.
- The second is to have a centralised dashboard, which is what the 2019 Bill suggests. The Committee had said that this method would have serious issues regarding interoperability, because one can't even imagine how many data fiduciaries take a user's consent throughout the day. So operationalising this will be slightly problematic.
  - Another method, to solve this problem, is for data fiduciaries to have their own consent dashboards and move on to a centralised dashboard over time. Again that would give rise to questions such as, "who is going to regulate these consent managers, right? Is it going to be sector specific? Is the data protection authority going to regulate all the consent managers?"

Is a consent manager a good idea?

Consent managers have worked fairly well for businesses and reduce the scope of a business slipping up and opening themselves up to liability, said a participant whose company has invested in consent managers outside of India. "Pilot results we have funded show that no matter what you do with privacy policies, people will not understand it. You simplify it, you put it in Hindi, nobody is going to understand it. It doesn't affect people's behavior and understanding, which is why consent managers are an interesting idea," the person said.

At the same, it might be concerning that "a brand-new concept has been introduced in a primary legislation, when it hasn't been sufficiently stress-tested elsewhere," another participant said. The speaker noted that the the RBI's Account Aggregator framework — the closest parallel to the proposed consent managers — took years to take off. "Although the regulatory framework went live in 2016, MeitY came up with electronic consent artefact, which the RBI then adopted. *Then* the RBI put out regulations saying that Account Aggregators need to function in user interest, that they're just a pipeline, an intermediary. They can't collect consent and pass it on, it just sits in the middle to makes the user's life easier," the speaker highlighted.

Another speaker was much more cynical: "But it's worth thinking as to why would a user put all their data in one place, or give access to all their data to

one data fiduciary? It's like putting all your money in one bank. What if the bank gets robbed?"

Do we really need it? How can it be better?

Maybe not. But maybe we need more clarification.

"Deleting it from the Bill might be as such as bad idea," said the speaker who pointed out the issues with Account Aggregator framework. Another speaker said, "It's too unclear if consent manager will just be a pipeline. It may actually be holding user information in escrow for other companies or platforms." And if this is the case, "then having a certification, protection, clarificatory framework on the dos and don'ts of a consent manager would be helpful," the speaker said. Another speaker also highlighted the concerns with a manager, and how its activities could be restricted:

> "Maybe more specifics, such as protective frameworks, could come through sectoral regulations, as the RBI has done with AA — such as who can and cannot be AAs, what they can do, meeting the net worth limit. Is the manager just meant to be a conduit for managing consents, will the user do their own analysis? If you give consents to say for X amount of time to Y companies of a certain category, can the companies use the data to cross-sell certain or advertise certain products to you?"

What about consent managers being significant data fiduciaries?

There are several models that companies can follow, a speaker said, taking the example of a UK-based consent manager, which is both the data manager and consent manager. "This consent manager manages the data on behalf of the consumer and stores it in different places. In that case, the company would be a very, very significant data fiduciary." But there are also lighter models "where the manager is just a pipeline, and doesn't handle storage. So the extent to which a consent manager will be a data fiduciary depends on the DPA's regulations on who qualifies as a consent manager and who needs to register." Another concern is that if a third-party — the consent manager — is managing the user's consent, the company would also need to know where their liability ends, and the manager's liability begins.

How would companies' intellectual property rights be be affected by government access to non-personal data?

The non-personal data is a huge deviation from the 2018 Bill, which had said that there should be a separate legislation for non-personal data, said one of the speakers. "This is the exactly where the 'data is oil' aspect comes in, pointed out another speaker. "Just as oil found on private land is not private, but is the State's, the argument here is also that data belongs to the government, and it can take it over. This is a very problematic way to look at non-personal data."

> "The scope of non-personal data is very large, there's a lot of data gathering companies do, and the information give them competitive advantage over others. Will corporations continue to invest in developing this kind of data and analytics, only to part with it when the government asks for it? This will definitely stifle innovation." — a speaker

---

Read Part II of our notes from the session on user rights and data fiduciaries here. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.