#NAMA: Looking at how well the Personal Data Protection Bill, 2019, protects user rights

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

Does the Bill do enough for user rights? Does it live up to Puttaswamy standards?

It's a good thing that right to erasure is there, the rest maintains the status quo as the 2018 Bill, said a speaker. It's commendable that most rights under the Bill are the same as the ones in GDPR. It boils down to how regulations around the functions of the Adjudicating Officer would work, a speaker said.

The Bill is all right when it comes to private companies, but not when it comes to protecting users from the government, according to multiple people:

- **"Individuals should have been allowed to make complaints and carry out legal proceedings, rather than leaving it to the DPA.** This was a similar issue with Aadhaar, where only the UIDAI could decide what complaints to take up. The Bill is all right in terms of rights, but the large carveouts made for government, the data localisation business, and critical personal data may have to be tested again in a court of law. The Bill complies with the Puttaswamy standards, **but not when it comes to government exemptions**."
- "The Bill fares well with respect to private companies to ensure individual rights. **But it fails in respect of protecting individual rights vis-à-vis the State.** The blanket exception to processing data without consent for state functions is extremely troubling. A law cannot be based on

> exceptions, it has to based on rule, and exceptions have to be granted *in exceptional situations*."

One of the problem areas in the Bill is the excessive distinction and hierarchy between the state/government as data fiduciaries and the private players as data fiduciaries, said another speaker.

Using ambiguity to the government's benefit

According to a lawyer, **Section 35 appears to be "drafted very cleverly"** and **"there might just be enough for it to by-and-large be constitutional.** It's worrying that the government has access to that kind of information, and the power to exempt itself to such a large extent," they said.

> "At the same time, the law has beautiful qualifying words. For instance, 'necessary or expedient'. But we have no idea what is necessary or expedient because there is no jurisprudence. The grounds on which they are talking are the same as the ones in Puttaswamy, or the Constitution under which any fundamental right can be restricted, such as 'may, by order', 'notify in writing', direct at this law shall not apply to any central, to any particular agency."

An audience member pointed out that "it's a serious problem that the Bill is government heavy, and not user-heavy. The DPA's job is to mediate between users, government, and industry, but it doesn't have enough structure to be able to that."

Does the Bill protect users from private entities?

Yes, according to one speaker: "It doesn't get better than this when you look at privacy law internationally, including GDPR."

- "A lot of detail will come through in the DPA's delegated legislation, which is why it's important an open consultative process, and conversation with industry to understand best practices in cyber-security and encryption for example," said a speaker.
- The Bill is progressive as far as you exclude the government exemptions portions of it. It's like an iceberg at this time, the DPA's regulations will define the rest, said another speaker. "Agency can be given to the user such that they have the ability to pursue action against bad actors," they added.
- "There might to be some regulatory capture of the DPA, because the eligibility criteria of the DPA's members has been diluted to bits. It's unclear to what extent the DPA will be open to suggestions from consumers and consumer advocates," said another speaker.

How would data portability be operationalised? How would it impact companies' intellectual property?

Right to data portability is the a user right under Bill, but there is a concern that it would impact intellectual property of private companies, according to a lawyer with expertise in intellectual property rights.

"While right to data portability is a fair right, how would the line between data generated about me versus data generated about me using proprietary algorithm be drawn?" asked another speaker. "It's a company's entire business model and intellectual property. How would we ensure that technology companies are not penalised for using their proprietary materials on user data?" they queried. According to another speaker, the Bill is cognizant of this, as it specifically mentions that the only exception to the rule about data portability is if it impacts trade secrets, which has a higher threshold than copyright.

"Whatever I create in a machine-readable form will not just be a compilation, but some intellectual input will go into it; and companies will necessarily create something proprietary, and that can be protected under the Copyright Act. This is the data which companies have competitive advantage on, and the trade secrets exemption is not enough," another speaker highlighted. Besides, right to data portability may also infringe on another person's personal data privacy, noted a participant.

How does right to data portability safeguard data of other users? Does it account for their consent?

An audience member asked how the bill would deal with a situation where a user porting their data is also pulling their entire social graph which has other users' data, even possibly sensitive personal data, along with their own. How would the new platform deal with this, since they haven't taken the consent of the other users, the audience member asked.

"The language in the Bill creates this challenge," said a lawyer in response. "If data portability were to be associated only with data that I have provided the platform by myself and that data had to be ported, it wouldn't really be an issue. However, now the platform has to port data it received from me, but also information *associated* with my profile, as well as any data *it has generated about me*." The Bill doesn't solve for this yet, the lawyer concluded. Another speaker said that it remains to be seen how consent would be dealt with in this situation:

> "GDPR has a provision on how entities are required to deal with data that they did not get access to directly from the user themselves, but that's absent from this Bill, but this question should definitely be posed to the regulator as to how rights of ancillary users protected."

How will portability work between industries, since there isn't standardisation?

One can port data from telco to telco, but how can one port data from Orkut to a hospital or telco?, asked a audience member.

Again, "the Bill doesn't envisage this, although that's what a user is more likely to do", the Bill says the fiduciary has to make user data available to them in a commonly used and machine-readable format. "But it doesn't say anything about whether two telecom operators, or two social media companies should be able to access it. It's sector and industry agnostic. The Bill envisages, in spirit and principle, that a user has to be empowered enough to take their information from one platform to the other," said the speaker.

Would right to data portability apply to eKYC?

There are already provisions for a central KYC repository, said a lawyer who has worked on financial services.

> "So if I open an account with ICICI Bank, and do my KYC with ICICI Bank, the bank has to deposit that information with CERSAI. Later if I want to open an account with IDBI, I just have to quote one number, a KIN number, then IDBI Bank can access my KYC data from that central repository," the lawyer said. "This is also incorporated by the RBI and its master directions on KYC," the lawyer concluded.

Dealing with data breaches

It's unfortunate that the DPA will decide whether or not to notify a data breach to data principals, and that the data fiduciary has to take its permission, said an audience member. But the reason for this may be to ensure that a notification may be to balance bad actors from taking advantage of a breach, said a speaker. "In any case, the DPA is holding our rights in confidence, but it's ability to do so is doubtful," the speaker said.

From what some members of the Joint Parliamentary Committee have been saying, "the delayed notification means the company has to tell the customer about a breach, when the DPA believes that you must, but the company can always tell the customer in the interim."

Why the central government deciding what's sensitive personal data is an issue: An audience member said they found it "considerably troubling that you [the government] decides what is sensitive data for me". "A person of a religious affiliation may not want anybody to know what kind of movies they are watching, for example. Some people like to show off where they travel to, others for security reasons may not want that to be known," they said. And this why "any data breach, any disclosure should be notified to whoever the data belongs to, by default. So, we should not get into the trap of what is sensitive and what is non-sensitive,' the person said. The Bill allows the Central government to notify other kids of data as sensitive personal data in addition to the 11 listed categories.

Other issues

DISHA to stay? The Health Ministry said a month ago that it's scrapping DISHA because discussions on health data will be subsumed within the Personal Data Protection Bill. DISHA will go, but the larger principle on sectoral regulators will very much continue to be in place.

Porting health data in emergencies: Prime facie, an individual has the right to access all their information, and in cases of emergencies, one hospital can request another hospital for information. Let's say X Hospital has my data and I'm now going to Y Hospital in an emergency, X Hospital now no longer requires my consent if it is an emergency situation to transfer that data to Y Hospital. The PDP Bill is a sector-agnostic principle-based bill, so sector-specific regulation may be created by the Health Ministry at a later stage.

Conflict with Digital Health Blueprint: "The National Digital Health Blueprint is a purely technical document, but talks about electronic health records, sharing of electronic health records, setting up a new authority that's going to oversee this entire framework, so on and so forth. It talks of the user owning their data, but the Bill has no such concept of ownership. The Blueprint talks of about data being owned by the patient for their lifetime, but per the Bill, users can erase their data, so they are totally at conflict. If the principal legislation says you can erase data and the other legislation or the subordinate one wants data to be preserved for the lifetime of a person and longer, there's a fundamental conflict," an audience member said.

Scope for self-regulation: The DPA can choose to recognise codes of practices, including those by industry, to be part of the regulations. The Authority will prescribe the codes of practice. Any scope for for self-regulation or industry participation will be at the level of stakeholders interacting with the DPA.

What's lawful processing under the Bill? What is lawful processing would be a combination principles such as free and fair processing, principles around transparency and data minimization, etc, and then on the consent-based framework, and ways of data collection, etcetera.

Is a missed call campaign by a political party. Can a missed call qualify as consent? Are political parties data fiduciaries? A missed call is a grey area, but it would not qualify as consent, since consent has to be free, fair, transparent, among other things, per the Bill. The user has to very clearly know why their data is being used, how will it be processed, what are the probably significant consequences and harms. The Bill also says that inferred consent is not explicit consent.

Read more: *Personal Data Protection Bill, 2019: Looking at social media intermediaries and siginificant data fiduciaries*

What can be better

Our speakers recommended the following steps to make the Bill better in terms of protecting user rights:

- **Clear, specific, transparent regulation**:
  - There should be clear and specific regulations from the DPA.
  - There should be a transparent process for delegated legislation where businesses and start-ups can get involved. There should be an open consultative process, white-paper approach each time the DPA makes one of the 40 decisions under the Bill.
- **Specify DPA's powers**: The Bill should also lay out detailed manuals the DPA's executive process on licensing and investigation. For example, the US has a 1,275-page document and SoP on how to investigate banks; the RBI has no manual, which means it can literally do anything it wants to do.
- **Engage with industry on non-personal data**: The requirement for requisitioning of non-personal data can be improved by creating a procedure for engagement, wherein a data fiduciary may respond to such a request, either to clarify its stance regarding feasibility or for any objection it may have. Currently, there is a specific requirement for compliance with all directions of the DPA, which is highly and heavily influenced by the Central government.

Read Part I 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.