#NAMA: Improving the Personal Data Protection Bill, 2019, to safeguard against surveillance

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 from 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 government access to data. Read Part I here.

Potential safeguards against surveillance in the Bill

There are potentially two safeguards against broad surveillance and unwarranted government access to data as given under Section 36, according to a speaker:

1. **Section 4** [Prohibition of processing of personal data except for "specific, clear and lawful purpose"]: Section 36 does not exempt the operation Section 4. The requirement for clarity and specificity might obviate some of the broadness that comes with this kind of surveillance.
2. **Section 92** [Bar on processing certain forms of biometric data]: This section prohibits the processing of biometric information except when permitted by law. There are very few statutes that explicitly authorise the processing of biometric information — Aadhaar Act and Identification of Prisoners Act, 1920 that permits people to be fingerprinted when a person is arrested.
   However, if the exemption is granted under Section 35, that's a "wholesale exemption" which is a more difficult situation, they clarified.
3. **DPA is crucial to curtailing government access to data:** According to the Bill, government agencies are also data fiduciaries and have responsibilities that a data fiduciary would have. But they can be relieved of most, if not all, of their duties through exemptions under Section 35 and Section 36. However, a speaker pointed out that this would be governed by the efficacy of the Data Protection Authority (DPA). "With this Bill,

we have vested all our faith in the DPA to keep us safe from any privacy violation. But if the DPA itself is ineffective or compromised, nothing will work," a speaker said.

DPA's functioning would be determined by how independent it is, but under the latest draft, it is executive committee. Unlike the 2018 Bill, there are no judicial members. As a result, the DPA will effectively be controlled by the government, and thus its effectiveness remains a fundamental question, the speaker said. But, as a speaker pointed out, "the whole point is that the central government is the first violator".

"We saw this happen with the Cyber Appellate Tribunal under the IT Act. When one of the chairpersons retired, the government did not appoint any one new and just kept the post vacant. And thus the Tribunal became essentially non-functioning." — a speaker

Greater oversight over access, curtail exemptions: Recommendations

1. **Make the objective and preamble of the Bill unequivocally about data protection:** "The Preamble of the Bill needs to unequivocally state that it is for the enforcement of administration of the right to privacy of all individuals. The digital economy equivocation has to go. How would we feel if the Domestic Violence Act said that it is meant 'to prevent violence against women and to preserve family values'," a panelist railed.
2. **State should be the model data controller:** The Statement of Objectives of the Bill should say that the State will be the model data controller. Also, a speaker said that the term 'data fiduciary' has to go as it deprives users of their agency. "Data controller is a much better functional term," they offered.
3. **Judicial review of access to personal data by government agencies:** Just as the Srikrishna Committee had recommended in its report, there should be prior judicial review of State access of personal data. "This can de done through a designated court or judicial members in an independent authority such as the DPA," proposed a speaker. This includes an appeal mechanism against the decisions of this judicial body, and ex-ante and ex-post reporting mechanisms.
4. **Oversight mechanisms to make State agencies accountable:** "Oversight bodies should be identified which monitor the working of State agencies," a speaker said. Such bodies should release periodic reports with details about the functioning of these agencies, data fiduciaries which constantly get requests for personal data, and the number of requests they receive.
5. **Amend the Bill to curtail exemptions under Section 35:** When it comes to inclusion of four more grounds to blanket exemption for agencies under Section 35, speakers generally opposed the move and said that the

Bill needs to be amended to define terms such as 'national security', 'public order' narrowly.

6. **Notify users**: Deferred notice should be sent to data subjects, a panelist said. "This should be followed by right to redress," they said. There should also be a means to notify the user if there is any kind of unlawful surveillance, another speaker proposed, both by the private companies and by the State.
7. **Evidence from surveillance that was not a proportionate response be inadmissible:** Taking a leaf out of the Bombay High Court judgement on evidence collected from disproportionate surveillance, a speaker suggested that information that is obtained from surveillance which does not conform to the proportionality standard of the Supreme Court should be decreed unconstitutional and not be admitted in court.
8. **Appoint Data Protection Officer for State agencies:** "Law enforcement agencies and agencies accessing this kind of personal data should have a data protection officer which goes through interception warrants and data requests, and make sure that they adhere to the law, and have least restrictive measures," a panelist suggested.
9. **Need for whistleblower protection:** Although whistleblower protection was not discussed by the Justice Srikrishna Committee, it is required in light of revelations about the NSO Group-Pegasus scandal where it is a clear that a government agency purchased it, but its identity remains unknown, a panelist said. "We have a Whistleblower Protection Act, but it has not been brough into force, and even that does not do enough," they argued.
10. **Have a separate law to implement surveillance reform:** "We need a separate law that gives intelligence agencies a statutory basis for their existence itself," a speaker said.

Read Part II and Part III of our notes on government access to data. Read our coverage of the discussions here: #NAMA – India's Data Protection Law – January 2020.