Personal Data Protection Bill, 2019: Protecting children's data online

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the fifth article in the series. Read our extensive coverage of the Bill here.

By Smitha Krishna Prasad

Decades after the first data protection laws were implemented, we still continue to struggle with some of the basics of personal data protection — how should personal data be defined? Corollary to this, is the question of whether some personal data matters more than others.

Many privacy scholars now agree that the relevance and sensitivity of personal data should be determined by context. The idea is to protect individuals or groups of individuals in contexts where certain personal information makes them more vulnerable. Implementing this kind of protection under the law however, has not been as easy given how often 'context' and therefore sensitivity changes. The compromise that many lawmakers have found seems to be the categorisation of personal data and sensitive personal data – all data is to be protected, but certain types of data are sensitive irrespective of context and require increased protection. The brand new Indian Personal Data Protection Bill, 2019 (PDP Bill), also uses this approach, and lists out a number of categories of data as 'sensitive personal data'.

While it is debatable whether sensitive personal data should be listed out, or a more dynamic approach is better — one of the few areas where there is consensus that additional protections are required irrespective of context, is in the case of personal information of children.

In this article, we look at what the PDP bill says about collection and processing of children's personal data, what this actually means in practice, and how this stacks up against global or best practices.

Chapter IV of the PDP Bill deals with the personal data and sensitive personal data of children. It provides for a broad requirement that data fiduciaries must process personal data of children in a manner that protects the child's rights, and is in the best interests of the child [Section 16(1)]. The rest of the chapter can be divided into two sections – the first, the provisions that go into when and how consent should be provided for the processing of such data, and who can provide such consent. The second issue this chapter focuses on is specific types of processing that will not be permitted in relation to children's personal data.

The PDP Bill considers any person below the age of 18 a child, in line with Indian laws on the age of majority, which require a person to be 18 years of age

to enter contracts, vote etc. In this context, it is not surprising that one of the areas of focus in the PDP Bill's discussion on children and children's rights in the context of personal information is the issue of consent, that is, a contract between the data fiduciary and the person providing the consent.

What happens when children want to access online services?

First, the data fiduciary must verify the age of the child, and ensure that consent is obtained from the parent or guardian. The PDP Bill itself does not go into detail on how this is to be done — except that there will be regulations on how age verification is to be undertaken. In prescribing these age verification mechanisms, a number of criteria will be taken into consideration, including: the volume of personal data processed; how much of that personal data is likely to be that of a child; and whether it is possible that there will be any harm to the child from the processing of such personal data. Regulations will also classify data fiduciaries that operate commercial websites or online services directed at children, or process large volumes of personal data of children, to be 'guardian data fiduciaries'.

How will the PDP Bill affect apps like PUBG?

At this stage, while we will have to wait to see what the regulations look like, it is likely that services popular with younger age groups, will at least need to implement age verification mechanisms, if not act as guardian data fiduciaries. A good example here would be gaming apps — these are sometimes targeted specifically at children, but many of the more popular apps are widely used by children and adults alike. A risk of harm to children using these services also may exist, leading to the classification of such service providers as guardian data fiduciaries.

While in the past we have seen some extreme reactions to such services, such as the recent ban on PUBG, a gaming app that is popular globally, and popular specifically among children, might need to tweak some services under the new PDP Bill. First, age verification and consent mechanisms will need to be modified. The age of consent specifically for online services is higher in India than in many other jurisdictions – the US and the UK for instance allow children between the ages of 13 and 18 to provide consent for some services, often depending on the competence of the child to consent. However, India doesn't seem to be adopting this system of differentiated ages of consent, except in the case of data fiduciaries providing counselling or child protection services to a child, in which case no consent is required from the parent or guardian.

The PDP Bill calls for a consent manager system to be implemented, in order to battle some of the common problems we see with the informed consent system. It may be worthwhile to look at whether this can be used as a specific solution in the case of children's consent as well. However, given that there is little

information on what the role of consent managers will be, or how age verification systems will be implemented, we may need to wait until the data protection authority starts discussing regulations to engage more on this subject.

What can be effective age-gating mechanisms?

The kind of age verification system that needs to be adopted, will be discussed in more detail in the regulations. Implementing effective age verification systems is an ongoing problem, given that some of the simple age verification systems are often easy to circumvent. The same case can also be made for systems in place to obtain the consent of the parent or guardian, once it is established that the personal data of a child is being collected.

A popular solution for this purpose is to implement knowledge-based tests. For instance, an age verification system that relies on arithmetic tests, could in theory verify the age of the person consenting, if there is an expectation that children will not be able to make such calculations – but this may not be the case for older children. However, more extensive knowledge-based tests often end up collecting more personal data than required – it is important to keep in mind that data protection principles need to be applied to this testing system itself.

What will happen if a guardian data fiduciary defaults on its responsibilities?

The second requirement under Chapter IV of the PDP Bill is applicable specifically to 'guardian data fiduciaries' – these data fiduciaries are not permitted to engage in profiling, tracking, behavioural monitoring of children or direct targeted advertising at children. They are also barred from undertaking any other activities that may cause significant harm to a child. This provision is likely meant to address situations like the recent case in the US, where Google/YouTube was fined USD 170 million for knowingly profiting from the use of personal data of children by directing targeted advertising at them. Similar to the consent requirements, an exception may be made (in the regulations) for data fiduciaries that offer counselling or child protection services.

Under the PDP Bill, any violation of the provisions of Chapter IV could result in a penalty up to INR 15 crore or 4% of the worldwide turnover of the data fiduciary for the preceding financial year (whichever is higher).

Is Chapter IV of the PDP Bill enough?

As discussed above, it is important that children have additional protections against the processing of their personal data, especially where such processing goes against their interest. To this end, the two broad purposes of Chapter IV of the PDP Bill — (i) ensuring that age verification mechanisms are in place, and

(ii) barring the profiling and tracking of children, the monitoring of children's behaviour, and targeting of advertisement to children — are commendable.

However, a few issues jump out immediately on the reading of these provisions. Some may be fixed by restructuring the provisions of the PDP Bill, but others possibly require a more thorough understanding of children's rights.

1. The first issue, is the idea of guardian data fiduciaries — the purpose for this classification appears to be to identify those data fiduciaries that are more likely to be processing children's personal data, resulting in harm to such children. However, the concept of guardian data fiduciaries is not really put to use beyond such classification. They have no additional obligations, other than the bar on profiling, tracking and monitoring of children's data, and targeting of advertising towards children, and other processing that may cause significant harm to children. It is not clear here why this bar is limited to guardian data fiduciaries — are those data fiduciaries that don't meet this threshold then allowed to engage in these activities that may result in significant harm to children?
    - It may be more useful to equate guardian data fiduciaries to significant data fiduciaries under the PDP Bill — undertaking some of the additional compliances applicable to significant data fiduciaries, such as data protection impact assessments may help identify harms to children, and then ways to protect them, better.
2. Second, the issue of differentiated ages of consent and the definition of what causes harm to children. With children of all ages using technology, and particularly online services, it is important to acknowledge that there is a sliding scale of sorts when it comes to harms to different age groups of children. This has been recognised by the National Commission for Protection of Children's Rights, which provides separate guidelines to 'older children' in its guide to online safety of children. It is important in this context, to look at children's data protection under the PDP Bill, from the larger lens of children's safety, as well as the agency and rights of children. For instance, it is important that the consent of a guardian or parent is obtained before a 10-year-old is able to access an online service, and provide personal data to the data fiduciary. However, there may be different concerns at play in protecting a 17-year-old, who may require privacy protections not only from the data fiduciary, but parents and guardians as well. While the exception for counselling and child protective services is useful in this context, practical concerns regarding the accessibility of such services and the relevance of harm in these contexts need to be accounted for.
3. Third, the absence of sensitive personal data in the discussion of children's data. Although the title to chapter IV indicates that it addresses sensitive personal data of children, Clause 16 itself has no mention of sensitive personal data. There will undoubtedly be situations where the sensitive personal data of children will need to be processed by a data fiduciary. It is important that this is accounted for and addressed under the law.

*
Smitha Krishna Prasad *is Associate Director at the Centre for Communication Governance, National Law University Delhi.*

Edited by Aditi Agrawal