Personal Data Protection Bill, 2019: Considering consent and offences

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 first article in the series. Read our extensive coverage of the Bill here.

By Rishab Bailey and Vrinda Bhandari

The popular teahouse chain Chaayos has been in the news recently for using facial recognition technology ('FRT') at a number of its stores in Delhi and Bangalore. Chaayos uses this technology to create profiles of its customers. These profiles are then used to "remember" them on subsequent visits, enabling repeat orders and efficient payment.

It has been reported that Chaayos does not display any information about the use of the personal data (that is, the image) collected by the system, that there was no opt-out option presented to customers, and that there was no obvious way of deleting one's data from the system.

With the tabling of the Personal Data Protection Bill, 2019 ('Bill'), in Parliament, the use of FRT may soon be regulated. In this post, we examine how the Chaayos episode would have been treated under the draft Bill, with a view to understand how the law proposes to deal with the issue of consent and the possible penalties for breach of these provisions.

How is Chaayos classified?

To begin with, the Bill would consider Chaayos as a "data fiduciary'' since it decides the means and purposes of processing of personal data. The customer would be a "data principal''.

The data captured by the FRT system would constitute "biometric data'' as it includes "sensitive personal data'' ('SPD'). Due to the particular vulnerability that misuse of such types of data can result in, the Bill imposes certain additional obligations on entities that seek to use this category of personal data.

Further, Section 92 of the Bill empowers the government to notify certain categories of biometric data that entities are barred from processing altogether, unless specifically authorised or required to do so by a law. This would imply that while normally, biometric data such as images of one's face could indeed be processed by a company such as Chaayos, the government can prohibit such practices. The grounds on which such a decision will be based are however unclear from the bare text of the proposed law.

Proportionate obligations under the PDP Bill, 2019

In order to give individuals greater control over their personal data, the Bill grants data principals a number of rights and imposes concomitant obligations on data fiduciaries. However, in order to ensure that obligations on entities are proportionate to the risks involved and to ensure that entities are not overburdened by the law, the Bill imposes obligations in a graded manner.

Under Section 26, certain data fiduciaries can be deemed "significant data fiduciaries" based on factors such as the volume of data processed, the turnover of the fiduciary, the risk of harm, or the use of new technologies in the processing. These entities will then have to comply with certain additional obligations such as preparing data protection impact assessments, appointing a data protection officer, and ensuring annual audits by an independent data auditor.

On the other hand, Section 39 of the Bill excludes certain "small entities" from having to comply with the law, should they process personal data manually (for instance, through maintaining written records). Such entities will be notified by the proposed Data Protection Authority having regard to factors such as the turnover of the entity, the purpose of collecting the data and the volume of data being processed. Notified entities will not have to comply with a number of provisions in the law such as those pertaining to notice and data retention, user rights (of access, rectification and erasure, data portability and right to be forgotten), as well as the transparency and accountability measures (such as the need to put in place security safeguards or report data breaches).

In our example, given the use of biometric data and facial recognition technology, it is not inconceivable that Chaayos could be categorised as a "significant data fiduciary". It would then have to comply with the additional obligations mentioned above. This implies that companies will have to make a reasoned decision about their data processing practices, particularly for functions that are not strictly related to their business. Should they choose to introduce a range of new but not strictly necessary features, they will have to take on the costs of complying with additional obligations. That said, Chaayos will not be able to claim the exemption under Section 39, as it is clearly using automated technology to carry out the processing.

How does consent work under PDP Bill, 2019?

The PDP Bill requires a data fiduciary to only process personal data if it has a valid ground to do so. The most important aspect of this is obtaining the consent of the data principal. Section 11 of the Bill requires the data fiduciary to ensure that it secures "explicit'' consent of the data principal before or at the time of collecting SPD. The onus is on the entity concerned, which is Chaayos in our case, to prove it adequately secured consent.

But what does this entail? How does the law seek to ensure that the individual is properly informed and in control of their information?

How do these provisions work with the Chaayos hypothetical?

As per the Bill, in order for consent to be considered valid, it must be:

1. **Free**, that is, not induced by fraud, misrepresentation, coercion, undue influence or mistake. This implies that the data principal must not be forced or tricked into providing consent. She must be given a real choice about whether to provide the information or not. Thus, Chaayos will not be permitted to start recording the customer's image the moment she enters a store or picks up the tablet used for the FRT. The customer must first be given an option about whether to use the system or not.
2. **Informed**,that is, that the data principal must be provided the information listed in Section 7 of the Bill, that is, information pertaining to the purposes to which the data will be put to, the types of data being collected, information on how to withdraw consent, who the data will be shared with, etc. This information is to be provided in a clear and concise manner, that is reasonably comprehensible, and in multiple languages where necessary. This provision is important as it allows the data principal to understand the risks involved, and therefore make a rational choice about providing consent. In the context of SPD, the law also requires the data principal to be informed of any particularly harmful risks that they may be exposed to by allowing the processing of their data. In our hypothetical, Chaayos would have to provide the customer an easily accessible set of terms which provide her all the relevant information needed to decide whether to consent to the processing, as well as information regarding how to withdraw consent or make complaints to the company.
3. **Specific** consent given must relate specifically to the purpose of processing that is contemplated by the fiduciary. The consent clause must not be overly broad or ambiguous or encompass unconnected purposes. In the context of SPD, the data principal must be given granular choice, that is, the choice of making separate decisions regarding different categories of SPD that are to be collected and processed. Thus, Chaayos would have to provide information regarding the provision of the FRT system itself and the possible consequences stemming from using/not using the system. Their notice would also have to specify the types of information collected, who it would be shared with, the purposes it would be used for and so on. The challenge with this will be to ensure the notice contains all the relevant information without making it inaccessible to a common person. However, Chaayos could choose to use the model notices that the proposed Data Protection Authority will issue, thereby making it somewhat easier to comply with the law.
4. **Clear:** This means that the consent must be indicated through an affirmative action that is meaningful, given the context. In the context of SPD, the law requires express consent to be obtained, with specific additional "affirmative action" taken by the individual. There must be no doubt that the individual concerned wanted to consent to the processing of their SPD. Chaayos would then have to ensure that the customer specifically and ex-

pressly consents to the processing of their image — say by clicking on an empty check-box since mere silence or the use of pre-checked boxes will no longer be considered valid.

5. **Capable of being withdrawn:** This also involves ensuring that withdrawing consent should be comparable to the ease of giving consent. Thus, since the customer can give consent by ticking a box on a form, they should not have to send a physical letter to Chaayos requesting them stop processing the data. Additionally, it would be preferable if customer is given the option of sending an email to the company. The withdrawal of consent should also be followed by the deletion of her personal data that has been collected by the company, subject to any law in force.

Importantly, the data fiduciary cannot make the provision of any service dependent on the provision of personal data that is not necessary for the purpose.

How will this work in practice?

The draft Bill has introduced the concept of a "consent manager", who is a data fiduciary tasked with enabling the data principals to manage their consent, through an interoperable platform. Thus, the Chaayos customer can write to Chaayos, either directly or to the consent manager, to exercise her rights of confirmation, access, correction, erasure, and data portability. The withdrawal of consent can also take place through the consent manager.

The idea behind a consent manager may be to reduce the incidence of "consent fatigue", though how it will work in practice remains to be seen, and will largely be determined by the regulations that will be notified. Section 23(5) of the draft Bill states that the consent manager shall be registered with the DPA and be subject to various technical, operational, financial and other conditions, as may be specified by regulation.

What if you do not consent to the use of your image? Can Chaayos refuse to serve you tea altogether?

Under the draft Bill, Chaayos cannot outright refuse to serve you. The selling of tea itself is unconnected to the purpose of the processing of the facial image — which is to provide certain additional service features (such as repetition of orders, easier payments, etc.). Chaayos can, however, make access to these specific features dependent on the use of the FRT. They could therefore legitimately refuse to provide you the *convenience of choosing to repeat a previous order at one click*, but *cannot* refuse to serve you tea.

What if Chaayos refuses to follow the law?

The draft law seeks to ensure compliance by envisaging fairly stringent penalties. Data principals are empowered to make complaints to the company concerned, and if unaddressed can escalate them to the proposed Data Protection Authority

for redress. Further, the Authority can, on its own motion, investigate any untoward practices.

If subsequent to a hearing, Chaayos is found guilty of breach, it could be liable to pay a penalty extending to 15 crore or 4% of its global turnover in the preceding financial year. Further, it could be forced to pay compensation to a data principal who can demonstrate that she had suffered "harm" as a consequence of the illegal processing of her personal data.

Under the draft Bill, under Section 82, only the knowing or intentional re-identification of personal data, which has been de-identified by a data fiduciary/data processor, has been criminalised. The Bill departs from the Justice Srikrishna Committee version in three important aspects:

1. **It removes the offences of obtaining, transferring, or selling personal data and sensitive personal data contrary to the Act.** Under the 2018 version, if a customer's biometric data had been collected by Chaayos with their express consent, but later, any person had knowingly/intentionally/recklessly disclosed or shared this data with a third party, that person could be punished with imprisonment up to three years. This is not the case under the present 2019 Bill.
2. **Even for the offence it retains, that is, re-identification, the 2019 Bill removes the standard of "reckless" as a basis for criminalising certain actions.** Suppose all the SPD collected by Chaayos has been anonymised by it (although whether data can truly be anonymised to prevent re-identification is questionable). If some person, without the consent of Chaayos, intentionally re-identifies the data, they are liable to be prosecuted and punished. However, if the re-identification happens unintentionally, recklessly, or negligently, that is, if the person is not aware about the possibility of re-identification if two data sets were combined, but should have known; and hence, they ignore the danger and go ahead and combine the data set, then even if it leads to re-identification, no one can be criminally prosecuted.
3. **Only the Data Protection Authority is permitted to initiate criminal action for the offence under Section 82.** This is unlike the previous version of the Bill. This provision under Section 83(2) is similar to Section 47 of the Aadhaar Act, which was struck down by the Supreme Court in the Aadhaar Judgment, and had to be amended pursuant to the Aadhaar Amendment Act, 2019.

Overall, while the draft law does put in place a number of measures to ensure that individuals are given greater control of their personal data, it remains to be seen whether a consent based regime — however improved it may be from contract law standards — will actually change data processing practices for the better. Will consumers actually seek to take control of their data, including by taking the additional time to read privacy policies and make rational choices? Will they be able to successfully take action against companies that violate the provisions of the law? Only time, and perhaps the Regulations that will be

notified by the Data Protection Authority, will tell.

*

Vrinda Bhandari *is an advocate practising with the Delhi High Court, who works on issues concerning privacy, data, and digital rights.*

Rishab Bailey *is a fellow with the technology policy team at the National Institute of Public Finance and Policy, New Delhi. He has previously worked at a law firm, a software company, and with various civil society organisations on issues concerning technology policy and digital rights.*

Edited by Aditi Agrawal