Policy Brief

CUTS International
www.cuts-international.org

Key Definitions in the Personal Data Protection Bill 2019

Introduction

The Personal Data Protection Bill 2019 (bill),[1] warrants its functioning and implementation on key operational definitions. In this regard, various terms such as: 'personal data',[2] 'sensitive personal data',[3] 'critical personal data',[4] 'harm'[5] etc. have been defined under the bill. Some of these definitions suffer from ambiguities, and can result in broad and varying interpretations.

Clarity in the scope of these terms is pertinent to understand the expanse of the bill, with respect to rights of data principals (users), obligations of data fiduciaries (service providers), restrictions on cross-border data flows, offences, penalties and claims for compensation. Hence, evaluation of these terms in specific contexts becomes essential to assess the application of bill and its effect on various stakeholders.

Assessment of Definitions

Personal Data -

"personal data" means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

In its current form, the definition of personal data is contingent upon 'identifiability' of the person through such data. But, this criterion of 'identifiability' may differ depending upon the social, economic, cultural profile and intimacy of the person towards relevant data. This is also informed by the CUTS user perception survey on privacy and data protection, which observed that different users (based on gender, age, years of using internet etc.) perceive different information differently. For instance, female users are more uncomfortable in sharing their email-ids, compared to male counterparts or more adults are uncomfortable in sharing their personal photos compared to younger people.[6] Hence, it is important to consider user perspectives while determining 'identifiability'.

Also, the possibility of 'identifying' natural person may differ with relationship of such natural person with the relevant data. Consequently, absence of guidance to

determine 'identifiability' may result in varying interpretations and vagueness.

It might be useful to provide some identifiers and examples to elaborate on concept of 'identifiability' to make it more specific. In this regard, it will also be important to consider user perception with respect to different kinds of data, i.e. the test for establishing 'identifiability' should include a user perception and perceived sense of intimacy and necessity of such data. This was validated through our Privacy Survey. Similar identifiers are also provided within European Union's (EU) General Data Protection Regulation (GDPR).[7]

Sensitive personal data -

"sensitive personal data" means such personal data, which may, reveal, be related to, or constitute— (i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation; or (xii) any other data categorised as sensitive personal data under section 15.

The definition of 'sensitive personal data' specifies types of data such as financial data, health data, official identifier etc. The aim of categorisation of 'personal data' and 'sensitive personal data' separately is to provide more protection to certain types of data which are sensitive to the users. Although, this premise doesn't come out of the definition in a clear way, as it must also reflect users' perceived risk of misuse along with providing a guiding principle for categorisation of such data.

In this regard, being informed by the Chinese Cyber Security Law[8] and Japan's Act of the Protection of Personal Information (APPI),[9] a guiding principle of associated harm with revelation of data may be provided in the definition of 'sensitive personal data'. It can specify that the definition includes such data which if revealed can cause 'psychological, property or physical harm'.[10] Such specification will help categorisation of data through risks of such harm, justifying its sensitivity for the users.

Further, the definition excludes passwords from sensitive personal data. As observed in CUTS', survey, users don't use data protection tools making passwords their first and only line of defence for data protection.[11] Hence, **passwords should be reinstated within the definition of 'sensitive personal data'.**

Critical personal data -

"critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.

There is uncertainty in this definition, as there are no prescribed parameters for categorising such data. This results in wide discretion to the government for localising vast categories of data. **Seeking inspiration from the Information Technology Act, which lays down the meaning of 'Critical Information Infrastructure'[12], the definition may lay down specific parameters such as: *unauthorised collection, or breach of personal data which can have debilitating impact on national security, public health or safety should be given for critical personal data*.**

'Harm' -

"harm" includes— (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (iii) financial loss or loss of property; (iv) loss of reputation or humiliation; (v) loss of employment; (vi) any discriminatory treatment; (vii) any subjection to blackmail or extortion; (viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal;

'Harm' as prescribed in the bill lists certain outcomes which may cause adverse effect for users, but does not make a clear linkage to misuse of data. Further, the scope of the definition is limited as it does not take into account new risks which might have to be addressed with evolution of technology.[13] This creates ambiguity and confusion for users and service providers, and limits the rights of users to only listed harms. **To address this, the bill must provide a broader definition of harm, also appropriate guidelines regarding its interpretation to establish linkages with harms as listed to the personal data breach must be laid down. This could be done through specifying that such harm must be caused through processing of personal data or caused through personal data breach in contravention to the bill.**

1 The Personal Data Protection Bill 2019. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

2 S. 3(28) of the Bill

3 S. 3(36) of the Bill

4 S. 33 of the Bill

5 S. 3(20) of the Bill

6 Amol Kulkarni and Swati Punia, "Users' Perspectives On Privacy And Data Protection" (Jaipur: C-CIER, CUTS International).

7 GDPR , Article 4(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

8 Chinese Cyber Security Law 2017

9 Japan's Act of the Protection of Personal Information (APPI), https://www.ppc.go.jp/en/

10 Chinese Cyber Security Law 2017

[11] Amol Kulkarni and Swati Punia, "Users' Perspectives On Privacy And Data Protection" (Jaipur: C-CIER, CUTS International).

[12] Section 70 (1) "For the purposes of this section, —Critical Information Infrastructure‖ means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."

[13] Srikara Prasad, "An Analysis of 'Harm' Defined under the Draft Personal Data Protection Bill, 2018," *Dvara Research Blog* (blog), 2019, https://www.dvara.com/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/.