Baijayant "Jay" Panda
Member of Parliament
(Lok Sabha)
Kendrapara, Odisha

Member :
- Consultative Committee for the Ministry of Finance
- Parliamentary Standing Committee on Home Affairs

RO/2017-18/1421
October 5th, 2017

Mr. Arvind Kumar
Telecom Regulatory Authority of India
Mahanagar Doorsanchar Bhawan
Jawaharlal Nehru Marg
New Delhi - 110002

Subject: Consultation paper for Privacy, Security and Ownership of the Data.

Dear Mr. Arvind Kumar

Since i have recently introduced a private members bill in the Lok Sabha called Data (Privacy and Protection) Bill, 2017 the questions in your consultation paper are of relevance to me. The questions in your paper have been answered in regard with the bill as well.

I have annexed a copy of my bill along with your consultation questions. Hope the bill will be of significance in your endeavours.

Thank you.
Yours sincerely,

Baijayant "Jay" Panda

Annexures:
1. The Data (Privacy and Protection) Bill, 2017
2. CONTINUATION SHEETS : CONSULTATION PAPERS

NEW DELHI: 2, Mahadev Road, New Delhi-110001, India I Ph.: +91 (11) 23753430/31 I Fax : +91 (11) 23323355
BHUBANESHWAR : Plot 8, Bhoi Nagar, Bhubaneswar, Odisha-751012, India I Ph. : +91 (674) 2395551 I Fax : +91 (674) 2394954
E-mail : office@bjpanda.org I Website : www.bjpanda.in
@PandaJay @Baijayant"Jay"Panda

Office of Baijayant Panda
Consultation Paper for TRAI

Question 1. Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers? What are the additional measures, if any, that need to be considered in this regard?

No, the data protection requirements are not sufficient, for this reason Mr Panda has introduced a Private Members Bill (PMB) in the Lok Sabha called the 'Data (Privacy and Protection) Bill', which has been referred to in this consultation paper, and annexed at the end of this paper.

There is a need for stricter and better defined guidelines in cases of data collection, data handling, storage, removal of data, and finally the duties of those handling such data i.e. data controllers and data processors (DC/DP). There should be a duty on DC/DP in regards with taking consent and the duty of a DC/DP to take every customer through essential clauses of the Terms and conditions. In case of any breach, it is the duty of the DC/DP to inform the customer within a stipulated time period.

Question 2. In light of recent advances in technology, what changes, if any, are recommended to the definition of personal data? Should the User's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data? In particular, what are the new capabilities that must be granted to consumers over the use of their Personal data?

"Personal data" could be defined as any data or information which relates to a person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data. This will enable us to bring within its ambit personal data automatically generated through machine learning algorithms.

Yes, it is important that a users consent must be taken before sharing his/her personal data for commercial purposes and that consent should be express, affirmative and informed. It is important that the user's are taken through the essential clauses of the agreement in a simplified manner, so that they may

NEW DELHI : 2, Mahadev Road, New Delhi-110001, India • Ph. : +91 (11) 23753430/31 • Fax : +91 (11) 23323355
BHUBANESHWAR : Plot 8, Bhoi Nagar, Bhubaneswar, Odisha -751012, India • Ph. : +91 (674) 2395552 • Fax : +91 (674) 2394954
E-mail : office@bjpanda.org • Website : www.bj.panda.name

know the terms and conditions under which their data may be used for commercial purposes. The customers must be empowered with the knowledge to know where their data has been used. In case of a breach, the customer must informed be within a stipulated time period. The customer may also have the right to refuse giving his/her consent. Finally, there should be a provision for correcting data which is outdated or unwanted to ensure accuracy.
The matters regarding consent can be found in Section 5 to 15 in the PMB.

Question 3. What should be the Rights and Responsibilities of the Data Controllers? Can the Rights of Data Controller supersede the Rights of an Individual over his/her Personal Data? Suggest a mechanism for regulating and governing the Data Controllers.

The responsibilities of DC should be as follows:

1. The collection of personal data should be in a fair, lawful and transparent manner.
2. DC must maintain confidentiality and compliance with the rules of procedure.
3. DC must take adequate measures for fortification of data security against unauthorised or unlawful access or use, accidental loss, damage or any attack of cyber-attacks.
4. In case of a breach, it must be the duty of the DC to notify the affected person within 7 days.
5. It should be the duty of the data controller to maintain accurate records of data collected, accessed, stored and processed.

No, the agency of the customer over their personal data should always be paramount. DC can be regulated and governed by a quasi judicial body which may take suo-moto inspection of the Data controllers to assess compliance with the provisions of rules.

Duties and obligations of the Data Controllers can be found in Chapter V of the PMB.

Question 4. Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent? Will an audit-based mechanism provide sufficient visibility for the government or its authorized authority to prevent harm? Can the industry create a sufficiently capable workforce of auditors who can take on these responsibilities?

An audit based mechanism will be very necessary, where the powers to audit algorithms and the biases that may come in will lie with the quasi-judicial body. There will be a need for a sufficient workforce with sufficient knowledge of the field.

Question 7. How can the government or its authorized authority set up a technology solution that can assist it in monitoring the ecosystem for compliance? What are the attributes of such a solution that allow the regulations to keep pace with a changing technology ecosystem?

The provisions of an authorised authority have been explained in Chapter VII of the PMB, which talks about the Data Protection Authority.

The Data Protection Authority shall be constituted by the Central Government and shall be a quasi judicial body. The functions of the bench are as follows:

1. To adjudicate disputes and contraventions
2. To study and undertake impact assessment of rules pertaining to the subject matter
3. Consult with stakeholders on any issues pertaining the matters relating to the industry
4. Consult with the Central Government on matters of public importance
5. Suo moto initiate inspection of Data Controllers

Question 9. What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc? What mechanisms need to be put in place in order to address these issues?

While an overarching data protection regime should ensure high standard of data security, the only way to make it feasible will be that the liability to lie with the person and organisation who handle the data. The onus of data protection must be on the data handler or processor.
There is a need for separate sectoral practices but they must be in sync with technological advancements in the field.

Question 11. What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?
The various checks and balances in terms of surveillance can be found in Chapter VI of the PMB.
The exceptions where surveillance may be carried out should be under very narrowly defined exceptions. These exceptions have been listed below:

1. There can be no surveillance except according to rules prescribed under an act.
2. Any persons except a public servant or authority duly authorised by the Central Government to order or conduct surveillance or to assist in pending investigation by competent authority shall be barred from initiating, assisting or conducting surveillance.
3. The state shall have the power to collect, process, monitor and intercept personal data only in accordance with narrowly defined reasonable restrictions.
4. There has to be a time period prescribed for the surveillance period, and not carried on indefinitely.
5. Reasonable steps must be taken to ensure security of data collected during surveillance and maintaining confidentiality and secrecy thereof.
6. No targeted individual profiling can take place and this shall be deemed as violation of privacy.
7. There shall be no storage of surveillance which is not relevant, or after a period ofone year since the information was collected.

There is a need for greater Judicial participation on this front.

Question 12. What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

The different countries of interaction must have similar data protection norms as our country to uphold data security. Cross border flow of information needs strict monitoring, but is very important in today's digital and technological ecosystem to allow data companies to thrive.

NEW DELHI : 2, Mahadev Road, New Delhi-110001, India • Ph. : +91 (11) 23753430/31 • Fax : +91 (11) 23323355
BHUBANESHWAR : Plot 8, Bhoi Nagar, Bhubaneswar, Odisha -751012, India • Ph. : +91 (674) 2395552 • Fax : +91 (674) 2394954
E-mail : office@bjpanda.org • Website : www.bj.panda.name

As introduced in Lok Sabha

Bill No.100 of 2017

THE DATA (PRIVACY AND PROTECTION) BILL, 2017

BY

Shri Baijayant Panda, M.P.

ARRANGEMENT OF CLAUSES

Clauses

CLAUSES

CLAUSES

Bill No. 100 of 2017

THE DATA (PRIVACY AND PROTECTION) BILL, 2017

By

SHRI BAIJAYANT PANDA, M.P.

A

BILL

to codify and safeguard the right to privacy in the digital age and constitute a Data Privacy Authority to protect personal data and for matters connected therewith.

BE it enacted by Parliament in the Sixty-eighth Year of the Republic of India as follows:—

CHAPTER I

PRELIMINARY

Short title, extent, and commencement.

1. (*1*) This Act may be called the Data (Privacy and Protection) Act, 2017.

(*2*) It shall extend to the whole of India and, save as otherwise provided in this Act, it shall also apply to any offence or contravention thereunder committed outside India by any person.

(*3*) It shall come into force on such date as the Central Government may, by notification in the official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provisions to the commencement of this Act shall be construed as a reference to the commencement of that provision.

Definitions.

2. In this Act, unless the context otherwise requires,—

(*a*) "anonymised data" means data or information processed in such a manner that it no longer relates to an identified or identifiable person;

(*b*) "Authority" means the Data Privacy and Protection Authority constituted under section 44;

(*c*) "armed force" means any body raised or constituted pursuant to or in connection with, or presently governed by, the Army Act, 1950 (46 of 1950), the Indian Reserve Forces Act, 1888 (4 of 1888), the Territorial Army Act, 1948 (6 of 1948), the Navy Act, 1957 (62 of 1957), the Air Force Act, 1950 (45 of 1950), the Reserve and Auxiliary Air Forces Act, 1952 (62 of 1952), the Coast Guard Act, 1978 (30 of 1978) or the Assam Rifles Act, 2006 (47 of 2006);

(*d*) "authorised officer" means an officer, not below the rank of a Gazetted Officer, of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept a communication of another person or carry out surveillance of another person under this Act;

(*e*) "communication" means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

(*f*) "data" shall for the purpose of this Act refer to data as defined under clause (o) of sub-section (*1*) of section 2 of the Information Technology Act, 2000; 21 of 2000.

(*g*) "data controller" means a person who, either alone or jointly or in combination with other persons, determines the purposes for which and the manner in which any personal data are used, or are to be, processed;

(*h*) "data processor" with respect to personal data means any person. apart from an employee of a data controller, who processes data independently or on behalf of a data controller;

(*i*) "interception" or "intercept" means any activity intended to capture, read, listen to, record and/or copy communication of a person;

(*j*) "intelligence organisation" means institutions set-up under the Intelligence Organisations (Restriction of Rights) Act, 1985, the National Investigation Agency Act, 2008 and/or any other institution set up by the Central Government through an Act of the Parliament or the Executive for the purpose of collection, monitoring, processing and/or analysis of information relevant to national security. 58 of 1985. 34 of 2008.

(*k*) "person" shall for the purpose of this Act refer to an individual:

(*1*) "personal data" means any data or information which relates to a person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data;

(*m*) "prescribed" means prescribed by rules made under this Act;

(*n*) "processing" with respect to data, means obtaining or recording the information or data or carrying out any operation or set of operations on the information or data, whether or not by automatic means, including—

(*i*) organisation, adaptation or alteration of the information,

(*ii*) or data,

(*iii*) retrieval, consultation or use of the information or data,

(*iv*) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(*v*) alignment, combination, blocking, erasure or destruction of the information or data.

(*o*) "pseudo-anonymisation" means processing of personal data in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable person;

(*p*) "portability" refers to the extent to which data can be moved, copied, transferred or shared by any other means between different computers, computer networks, computer systems, and/or computer resource;

(*q*) "profiling" means any form of automated processing of personal data consisting of the use of personal data or information to record and classify behaviour of individuals to predict and analyse their daily activities for purposes other than promotion and marketing of goods and services;

(*r*) "surveillance" means any activity intended to collect, watch, monitor, intercept, or enhance the ability to do the same with a view to obtain information about a person, group of persons or class of persons through analysis of any communication, images, signals, data, movement, behaviour or actions;

(*s*) "sensitive personal data" means such personal information which consists of information relating to—

(*i*) racial or ethnic origins, political or religious views;

(*ii*) passwords;

(*iii*) financial information such as bank account or credit card or debit card or other payment instrument details or financial transactions records;

(*iv*) physical, physiological and mental health condition;

(*v*) sexual activity;

(*vi*) medical records and history;

(*vii*) biometric data relating to the physical, physiological or behavioural characteristics of a natural person which allow their unique identification including, but not limited to, facial images, genetic information, fingerprints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;

(*viii*) any details relating to clauses (*i*) to (*vii*) above as provided to body corporates for providing service; and

(*ix*) any of the information received under clauses (*i*) to (*vii*) above by body corporates for processing, stored or processed under lawful contract or otherwise:

Provided that any information that is freely and lawfully available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data for the purposes of this Act; and

22 of 2005

(*t*) "third party" means any person. public authority, agency or any other body other than the person whose data is collected or processed, the controller, the processor, and the persons who, under the authority of the controller or the processor, are authorized to process data or are recipients of the data so processed.

Application.

3. (*1*) This Act shall apply to—

(*a*) collection, use, storage, disclosure and processing of personal data or information of all persons through wholly or partially automated or manual methods;

(*b*) data controllers and data processors which are State entities, including Government agencies or authorised personnel on their behalf as well as private companies, partnerships or any other body corporate which conduct activities within the territory of India through a registered place of business or establishment, irrespective of whether data processing is carried out at such place or outside the territory of India; and

(*c*) data controllers and data processors which are State entities, including Government agencies or authorised personnel on their behalf as well as private companies, partnerships or any other body corporate which do not have a registered place of business or establishment in India and offer goods or services to persons in India, irrespective of consideration, as defined under the Indian Contracts Act, 1872, being sought *in lieu* of such goods or services. 9 of 1872.

(*2*) Nothing in this Act shall apply to collection or processing of data mentioned in Schedule I:

Provided that the Central Government may, by notification in the Official Gazette, amend Schedule I by way of addition and deletion of entries thereto :

Provided further that every notification under sub-section (*2*) shall be issued after consultation with the Authority and shall be laid before each House of Parliament.

CHAPTER II

RIGHT TO PRIVACY AND DATA PROTECTION

Right to privacy.

4. Notwithstanding anything contained in any other law for the time being in force, pursuant to article 19 and 21 of the Constitution and subject to the provisions of this Act, all persons shall have a right to privacy.

Express consent.

5. (*1*) No person shall collect, store, process, disclose or otherwise handle any personal data of another person, intercept any communication of another person or carry out surveillance of another person except in accordance with the provisions of this Act.

(*2*) For the collecting, processing, storing, disclosing and otherwise handling personal data, express and affirmative consent has to be obtained from the requisite person after full disclosure of information as required under Schedule II of this Act.

(*3*) Consent under sub-section (*2*) shall be considered valid only if it is freely given, specific, informed and an unambiguous indication of a person's intention to allow collecting, processing, storing, disclosing and/or otherwise handling personal data.

(*4*) Notwithstanding the above, consent may be overridden in cases where there is a legal obligation or medical emergency which is fatal or may likely lead to permanent or irreversible bodily harm as well as the reasonable restrictions mentioned in section 15:

Provided that any consent may only be overridden to the extent necessary and the person so affected shall be informed of the same.

Binding determination.

6. For the purposes of section 4, every person shall have the final and binding power to determine the manner in which his personal data is to be dealt with.

Person to be duly informed.

7. Every person shall be duly informed about the processing of information through issuance of a privacy notice which shall be concise, timely, updated, transparent, intelligible, written in clear and plain language (both English and vernacular language), be easily accessible and provided free of cost to persons with the information specified in Schedule II;

Provided that where consent is being sought with regard to a written declaration/ online form which contains other clauses and matters, the clauses or portions regarding the privacy notice should be clearly distinguishable from other clauses and matters.

Access to personal data.

8. Every person shall have access to his personal data which is collected, processed, used or stored by Data Controllers and Data Processors, including the right to obtain a copy and obtain confirmation that his data is being processed along with any supplementary information corresponding to the information mandated under Schedule II of this Act.

Rectification of personal data.

9. (*1*) Every person shall have the right to have his personal data rectified if it is inaccurate or incomplete.

(*2*) Every rectification under sub-section (*1*) shall be carried out by the Data Controller and/or Data Processor in the manner notified by the Central Government in consultation with the Authority as it may deem appropriate:

Provided that every rectification shall be completed within a period of sixty days of receipt of data for rectification.

(*3*) Any person who collects, receives, stores, processes or otherwise handles any personal data of another person shall, to the extent possible, ensure that it is not inaccurate or misleading and, where necessary, is kept up to date.

(*4*) No person who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the person to whom any personal data so collected, received, stored, processed or otherwise handled pertains, the opportunity to review it and, where necessary, rectify anything that is inaccurate, misleading or not up to date.

Seeking removal of personal data.

10. (*1*) Every person shall have the right to seek removal of personal data from Data Controller—

(*a*) where personal data is no longer necessary with regard to the purpose for which it was originally collected or processed; or

(*b*) where the person withdraws consent; or

(*c*) where personal data has been obtained unlawfully; or

(*d*) where personal data is required to be erased in accordance with a legal obligation pursuant to a Court order.

(*2*) Notwithstanding anything contained in Sub-section (*1*), removal of personal data shall not be allowed if there are overriding legitimate interests and it is necessary—

(*a*) in the interest of fundamental rights;

(*b*) for compliance of a legal obligation or court order or an any action taken by an officer in exercise of the power vested in him;

(*c*) for establishing or defending a legal claim;

(*d*) to safeguard public interest.

Illustration

If A, a convicted sex offender, seeks removal from the online sex offender registry maintained by the Government, the same shall be disallowed in light of the overriding public interest of safety of women and children.

Restrict processing.

11. (*1*) During the pendency of consideration of request for removal of specific personal data, the Data Controller and Data Processor shall restrict processing of the specific personal data of the person.

(*2*) It is hereby clarified that sub-clause (*1*) shall not restrict the collection/storage of personal data.

Data portability.

12. Every person shall, as and when required, receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to data portability to another data controller without any hindrance.

Breach of personal data.

13. Every person shall have the right to be duly and promptly informed, within seven days about any unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental) or other reasonably foreseeable risks or data security breaches of pertaining to their personal data.

Legitimate expectation of due diligence.

14. (*1*) Every person at the stage of giving consent for collection, processing, use or storage shall be have a legitimate expectation that data controllers and data processors shall abide by the provisions of this Act.

(*2*) Data Controllers and/or Data Processors shall take all security measures necessary for safeguarding and securing the personal data in their custody with due diligence.

Reasonable restrictions.

15. Notwithstanding anything contained in this Act, the right to privacy shall be restricted by the Authority in the manner specified by this Act for—

(*a*) reasonable safeguards for sovereignty or integrity of India, national security and for the defence of country;

(*b*) prevention of suspected acts of terrorism, corruption, money laundering, organised crime, sale or purchase of narcotic and psychotropic substances;

(*c*) investigation of cognisable and non-bailable offences under the Indian Penal Code. 1860 after a report has been duly filed under section 154 of the Criminal Procedure Code, 1973; 45 of 1860. 2 of 1874.

(*d*) investigation of any other offences under the Indian Penal Code, 1860, or any other Act for the time being in force, after an appropriate order has been obtained from the requisite judicial authority with regard to existence of probable cause and providing a fixed time-frame for such collection or processing; and 45 of 1860.

(*e*) maintenance of public order in situations of imminent danger of breakdown:

Provided that the above restrictions must be adequate, relevant, proportionate, not excessive in nature and must be imposed in the manner prescribed.

CHAPTER III

Methods and Principles of Data Collection and Processing

Collection and processing. etc. of personal data with prior consent.

16. (*1*) No personal data shall be collected, processed, stored, accessed or monitored without prior express consent of the person directly affected by such act.

(*2*) Consent should be express, affirmative and taken after information as mandated under Schedule II has been provided to the person in a manner which is clearly distinguishable, concise, timely, updated, transparent, intelligible, written in clear and plain language (both English and vernacular language):

Provided that every person subject to data collection shall be duly informed and be provided fair opportunity or mechanism to revoke consent at any time often has consent to the collection of personal data has been obtained:

Provided further that where the purpose of processing of data are changed or added or varied in any manner whatsoever, such additional data collection or processing which is in variance of the initial purpose shall not be done without the prior consent of the person.

(*3*) It shall be the duty of the data processor or controller to duly provide information and adequate explanation to the person while taking consent about the manner and extent to which personal data shall be accessed, collected, stored or processed.

Explanation.—For the purposes of this section "consent" shall have the same meaning and safeguards as provided under the Indian Contracts Act, 1872.

Special provisions for consent in case of minors and persons with disability.

17. (*1*) Notwithstanding anything contained in section 16, where the personal data belongs to a minor as per the Indian Majority Act 1875, the consent of minor shall be— 9 of 1875.

(*a*) obtained from a legal guardian; and

(*b*) duly verified by the data controllers and processors:

Provided that upon attaining majority, the minor shall have the right to either continue or terminate the consent given by the legal guardian on his behalf.

(*2*) In the case of differently abled persons, the data controllers and data processors shall make special provisions for providing privacy notices and obtaining consent in accordance with accepted standards and as per directions of the Authority.

Purpose of data collection and processing.

18.(*1*) Every data controller and data processor must duly notify every person of the purpose for which data is collected, accessed or processed in a comprehensive format and with the adequate information as provided under Schedule II of the Act:

Provided that in case of multiple purposes, each purpose shall be displayed separately and the ramifications thereof shall be provided to the person at the time of taking his consent.

(*2*) No personal data shall be collected, accessed or processed unless deemed necessary for achievement of the purpose specified under sub-section (*1*) and connected to the stated function:

Provided that if any other personal data is collected it shall be marked as "optional".

(*3*) Any additional or further processing of personal data for archiving or scientific or historical or statistical research, shall not be considered incompatible with the initial purpose if it is,—

(*a*) bona fide;

(*b*) in public interest; and

(*c*) subject to adequate safeguards.

Collection or processing of personal data.

19. Personal data of a person with his consent may be collected or processed lawfully, if—

(*a*) necessary for performance of a contract or at a stage immediately prior to entering into a contract;

(*b*) required in furtherance of a legal obligation;

(*c*) in case of a person's medical emergency;

(*d*) necessary for administration of justice pursuant to a court order:

(*e*) required for performance of any statutory, governmental or other functions by data processor or controller as duly specified to the person subject to data collection;

(*f*) necessary for the legitimate interests pursued by data controller or processor or the third party to whom data is disclosed after it is duly informed to the person:

Provided that the interests of data processors or controller or third parties shall be adequately balanced against any prejudicial effect of the same on the rights and freedoms of the person as guaranteed under this Act and under the Constitution of India; and

(*g*) required for any other purpose as may be notified by the Central Government in consultation with the Authority, from time to time.

Special provisions for Sensitive personal data.

20. Notwithstanding anything contained in section 16 or section 19 of this Act,

(*1*) Sensitive personal data shall not be processed unless express, affirmative and explicit written consent of the person subject to data collection has been obtained through letter or fax or email from the said person.

(*2*) No sensitive personal data under sub-section (*1*) shall be processed for any purpose apart from for the specific purpose for which it was collected and/or implementation of welfare schemes and social protection laws.

(*3*) If sensitive personal data has been collected by various government agencies, institutions, authorities or private companies, partnerships or any other body corporate. for a specific purpose or as a part of a statutory or legal requirement and any form of collaborating, converging or monitoring between or individually by entities shall be expressly barred if it amounts to or reasonably lead to —

(*a*) individual profiling except for circumstances of reasonable restriction as mentioned under section 15 of this Act; or

(*b*) mass profiling or profiling of certain group or class of persons without any lawful reason or adequate basis; or

(*c*) unlawful access by third parties.

(*4*) It shall be the duty of the data controller or processor, as the case may be, to ensure that the sensitive personal data is collected, stored or processed, in accordance with this Act with reasonable advanced security measures and safeguards to ensure the safety of such data.

CHAPTER IV

Transfer, Storage and Security of Personal Data

Prohibition on sharing of personal data.

21. No personal data shall be shared in contravention of the provisions of this Act.

Retention of personal data.

22. No personal data shall be retained after the achievement of purpose for which it was collected and has been duly completed up to the satisfaction of all parties:

Provided that nothing in this section shall apply to databases of sensitive personal data duly established by the Central Government or State Government, as the case may be.

Prohibition on prolonged or unnecessary storage of personal data.

23. (*1*) No person shall store any personal data of another person for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.

(*2*) Save as provided in sub-section (*3*), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

(*3*) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if —

(*a*) the person to whom it pertains grants his consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist; or

(*b*) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament:

Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith.

Transfer of personal data to third parties.

24. Any transfer of personal data to a third party shall be done pursuant to taking express, affirmative consent under Section 16 of this Act and after adequately informing them of the ramifications thereof in a comprehensive manner the requirements specified under Section 7 of this Act:

Provided that any transfer of data to third parties shall be done only after ensuring that the third parties' privacy policies and security standards are in no way less privacy preserving than that of the transferring party.

Cross-border transfer of personal data.

25. Any cross border transfer of personal data shall be done pursuant to taking express, affirmative consent under Section 16 of this Act and after adequately informing them of the ramifications thereof in a comprehensive manner the requirements specified under Section 7 of this Act:

Provided that any cross border transfer of data to any entity or person outside the territory of India shall be done only after ensuring that the privacy policies and security standards followed by such entity are in no way less privacy preserving than those prescribed under this Act.

Pseudo-anonymisation.

26. For collecting, processing, storing, disclosing and/or otherwise handling personal data, pseudo - anonymisation shall be encouraged as far as possible.

Notification of breach.

27. It shall be the duty of the data controller and data processor, as the case may be, in case of any breach, unauthorized access, destruction, use, processing, storage, modification, de-anonymisation, unauthorized disclosure (either accidental or incidental), or other reasonably foreseeable risks of personal data, to notify to the person who is the subject of such personal data as well as the Authority and take adequate steps to mitigate any harm or damage of the data security breach within seven days.

Security protocol.

28. It shall be the duty of the data controller and processor, as the case may be, to maintain adequate security measures and safeguards in accordance with the nature and form of security protocol as notified by the Central Government in consultation with the Authority, from time to time.

CHAPTER V

Obligations of Data Controller and Processors

Collection, etc. of data in a fair, lawful and transparent.

29. (*1*) It shall be the duty of the data controller or processor, as the case may be to collect, store, access or process the personal data in a fair, lawful and transparent manner and in compliance with the provisions of this Act.

(*2*) Any personal data obtained in contravention of sub-section (*1*) shall be deemed to be unlawfully obtained.

Responsibility of sharing and use of personal data.

30. It shall be the duty of the data controller or processor or third party, as the case may be, to ensure that all personal data is reasonably shared only when it is necessary, while maintaining confidentiality and in compliance with the provisions of this Act.

Fortification of data security.

31. It shall be the duty of the data controller or processor or third party, as the case may be, to take adequate measure for fortification of data security against unauthorised or unlawful access or use, accidental loss, damage, or any form of cyber-attacks:

Provided that in the case of a breach of data, it is the duty of the data controller or processor or third party to notify the affected persons within seven days of the occurrence of the breach as well as take adequate measures to mitigate any harm or damage:

Provided further that the burden of proof to substantiate that adequate measures are in accordance with the provisions of this Act, shall lie on the data controller or processor or third party, as the case may be.

Maintenance of accurate records.

32. It shall be the duty of the data controller or processor or third party, as the case may be, to maintain accurate records of data collected, accessed, stored and processed along with record of consent obtained as per the provisions of this Act.

Criminal liability.

33. Where a data controller or data processor or third party, as the case may be, has committed an offence under Chapter 8 which is punishable with imprisonment, every person in-charge of and responsible for the conduct of business shall, irrespective of direct commercial or financial benefit, incur criminal liability and be punished accordingly:

Provided that nothing contained in this Section shall render any such person in-charge liable to any punishment, if he proves to the satisfaction of the Authority that such offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

Appointment of Data Protection Officer.

34. (*1*) Every data controller or processor or third party, as the case may be, shall appoint a Data Protection Officer having adequate technical expertise in the field of data collection or processing and the ability to address any requests, clarifications or complaints made with regard to the provisions of this Act:

Provided that the data controllers and processors employing less than live hundred people and having a per capita turnover of less than one crore rupees may jointly appoint a Data Protection Officer, for resolving or addressing any requests, clarifications or complaints made herein in collaboration with other bodies with similar size or turnover.

(*2*) No additional fee shall be charged for resolving or addressing any requests, clarifications or complaints made herein.

Role of Data Protection Officer.

35. (*1*) The Data Protection Officer shall—

(*a*) act as an independent person;

(*b*) address requests, clarifications or complaints made in writing, including through electronic form, by any aggrieved person or legal representative thereof;

(*c*) take steps to initiate an inquiry and commence proceedings within seven days of receiving the complaint;

(*d*) resolve the matter within ninety days of receipt of complaint;

(*e*) recommend the data controller or processor to take action; and

(*f*) record the proceedings, the results thereof and the reasons for arriving at the decision in writing.

(*2*) In cases where the Data Protection Officer has not been appointed or is unable to or does not adequately resolve the complaints within the stipulated period of ninety days, the complainant may approach the Data Privacy Authority for redressal of complaints.

CHAPTER VI

SURVEILLANCE

Bar against surveillance.

36. Except for the manner provided in this Act and the rules prescribed thereto, no person shall conduct or assist in conducting any surveillance of another person.

37. Any person except a public servant or authority duly authorised by the Central Government to order or conduct surveillance or to assist in pending investigation by the competent authority shall be expressly barred from initiating, assisting, conducting or abetting any act of surveillance under this Act. Surveillance by private companies, partnerships or any other body corporate.

38. (*1*) The State has the power to collect, process, monitor and intercept personal data in accordance to the reasonable restrictions provided under section 15. Surveillance by the State.

(*2*) Any officer authorised by the Central Government, on the basis of information received or lawfully discovered by police, armed forces, intelligence organisation or any public official, if satisfied that the information sets out a reasonable threat to sovereignty, integrity, national security or defence of public order, he may forward the same to the concerned intelligence organisations.

(*3*) The concerned intelligence organisation shall, on receipt of information mentioned under sub-section (*2*), if deem necessary, seek an order from the Authority who may either reject or issue an order allowing surveillance or interception of personal data for reasons recorded in writing and addressed to concerned organisation:

Provided that the every case referred to the Authority under this section shall be processed and an appropriate order shall be passed within a period of sixty days of receipt of the case:

Provided further that the order should specify the communications or class of communications to or from the persons or class of persons that shall be subject to the order.

(*4*) For the purpose of sub-section (*2*), a Special division shall be set up by the Central Government for assistance of the Authority for determination of the cases referred:

Provided that prior to issuing the order, the Authority shall satisfy itself that all other lawful means to acquire the information sought to be intercepted has been exhausted and that the proposed interception is reasonable, proportionate and not excessive.

(*5*) The Special division set up under section (*4*) shall have the power to conduct preliminary investigation in the manner as prescribed by the Central Government, from time to time, submit their findings to the Authority who shall thereafter issue a detailed order to the intelligence organisation:

Provided that in case of military intelligence, which appears to be inaccessible or sensitive and/or confidential, the Authority shall consult the Cabinet Secretary, Government of India for the purposes of issuance of order under this section.

(*6*) After, receipt of order from the Authority the intelligence organisation shall conduct surveillance in accordance to the express conditions provided in the order.

39. Every order issued under section 38 shall specify the time period for carrying out the surveillance by the intelligence organisation of the personal data: Duration of surveillance.

Provided that if any extension is required for the surveillance, the intelligence organisation shall approach the Authority along with reasons for such extension.

40. Every State authority, intelligence organisation or private companies, partnerships or any other body corporate shall, as the case may be, which participate, assist, co-operate, conduct or carry out activity to facilitate surveillance pursuant to provisions of this chapter, take reasonable steps to ensure security of the data so collected and maintain the confidentiality and secrecy thereof. Security and duty of confidentiality and secrecy.

41. If at any stage, information or personal data obtained through surveillance is required to be produced in a court of law, the onus to prove that the same has been collected in accordance with the provisions of this Act while maintaining a proper chain of custody Admissibility in court.

without any tampering or external interference shall be on the concerned State authority, intelligence organisation or private entity, as the case may be.

No targeted individual profiling.

42. Any targeted profiling of individuals or of a certain section or class of persons without any basis and harassment, whether physical or financial or other means, shall be expressly barred and be deemed as violation of privacy under this Act.

Storage of surveillance.

43. No information or personal data that is collected in the process of surveillance which is not relevant for the purposes of evidence or for continuing investigation by the intelligence organisations shall not be stored by or accessible to the intelligence organisations after a period of expiry of one year from the date on which the order under which the information was obtained.

CHAPTER VII

DATA PRIVACY AUTHORITY

Constitution of Data Privacy Authority.

44. The Central Government shall, by notification in the Official Gazette, constitute an Authority to be known as the Data Privacy and Protection Authority for carrying out the purposes of this Act in such manner as may be prescribed.

Appointment of Chairperson and other members to the Authority.

45. (*1*) The Central Government shall, in consultation with the Chief Justice of India, appoint a Chairperson and other members to the Authority in such manner as may be prescribed.

(*2*) The Authority shall constitute of judicial members as well as technical members in equal proportion.

(*3*) A judicial member shall otherwise be qualified to be a High Court Judge or have been a member of the Indian Legal Services and have held a post in Grade I of that Service for at least three years.

(*4*) A technical member shall have expertise, special knowledge of and adequate professional experience in technology and processing/collection of data.

(*5*) The Chairperson of the Authority shall be the senior-most judicial member.

Constitution of Benches.

46. (*1*) Subject to the provisions of this Act, the Authority may, by notification in the Official Gazette, constitute Benches to exercise the jurisdiction, powers and authority conferred to under this Act.

(*2*) Each Bench shall consist of at least one judicial and one technical member of the Authority to be decided by Chairperson in such manner as may be prescribed.

(*3*) The Benches of the Authority shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Authority, by notification in the Official Gazette, specify.

(*4*) The Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Authority may exercise its territorial jurisdiction.

(*5*) Notwithstanding anything contained in sub-section (*3*), the Chairperson of the Authority may transfer a member from one Bench to another Bench for carrying out the purposes of this Act in such manner as may be prescribed.

(*6*) If at any stage of the hearing of any case or matter it appears to the Chairperson or a member of the Authority that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit.

Terms of office, conditions of service, removal of Chairperson and members.

47. (*1*) The Chairperson and every member of the Authority shall hold office for a period of five years or till the age of sixty-five years whichever is earlier:

Provided that no member shall be elected for more than two consecutive terms.

(*2*) The Central Government shall remove a person from the office of Chairperson or member, as the case may be, if that person—

(*i*) has been adjudged as insolvent;

(*ii*) has been convicted of an offence of moral turpitude or any other offence as may be deemed appropriate and notified by the Central Government:

(*iii*) has become physically or mentally incapable of acting as a member;

(*iv*) has acquired such financial or other interest as is likely to prejudicially affect completion of duties;

(*v*) has abused his position in such a manner that continuance in office shall be prejudicial to public interest:

Provided that no person shall be removed under this sub-section unless he has been given a reasonable opportunity of being heard in the matter.

(*3*) The salary and allowances payable to and other terms and conditions of service of Chairperson and members of the Authority shall be such as may be prescribed.

Procedure and Powers of the Authority.

48. (*1*) The Authority shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules.

5 of 1908.

(*2*) The Authority shall have power to regulate its own procedure including the place at which it shall have its sittings.

(*3*) The Authority shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely:

5 of 1908.

(*a*) summoning and enforcing the attendance of any person and examining him on oath;

(*b*) requiring the discovery and production of documents or other electronic records;

(*c*) receiving evidence on affidavits:

(*d*) issuing commissions for the examination of witnesses or documents;

(*e*) calling upon any data processor or data controller at any time to furnish in writing such information or explanation as may be deemed necessary;

(*f*) hearing and deciding matters where criminal liability is involved with respect to the provisions of this Act;

(*g*) issuing an order for search and seizure pursuant to a complaint or *suo-moto* if there is *prima facie* evidence of contravention or violation of this Act;

(*h*) reviewing its decisions;

(*i*) dismissing an application for default or deciding it *ex parte*; and

(*j*) any other matter which may be prescribed.

(*4*) Every proceeding before the Authority shall be deemed to be a judicial proceeding within the meaning of Sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code, 1860 and the Authority shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

45 of 1860.

2 of 1974.

Functions of the Bench.

49. The Authority shall,—

(*a*) adjudicate all disputes and contraventions of the provisions of this Act referred to it, impose penalties and punishments thereof;

(*b*) study and undertake impact assessment of Bills tabled before each House of Parliament, existing legislation, ordinances and rules pertaining to the subject matter of this Act as it deems necessary and make recommendations to the concerned Ministry;

(*c*) consult with stakeholders on any issues pertaining to the subject matter of this Act which are of public importance;

(*d*) consult with the Central Government according to the provisions of this Act; and

(*e*) *suo-moto* initiate inspection of **Data Controllers and Data Processors** to assess compliance with the provisions of this Act.

Filing of Complaints.

50. Any person aggrieved by the decision of the Data Protection Officer or not received any adjudication despite lapse of ninety days may file a written complaint with regard to non-compliance, contravention or any other violation of this Act before the Authority:

Provided that where the Data Protection Officer is not appointed, the person may directly approach the Authority.

Issuance of orders.

51. The Bench shall upon adjudicating the complaints referred to in section 50 award fines, call for directive or injunctive measures, compensation and/or imprisonment of such term as it may deem appropriate.

Appeal.

52. An appeal against the decision of the Bench shall lie to the Telecom Disputes Settlement Appellate Tribunal set up in accordance with the provisions of the Telecom Regulatory Authority Act, 1997. 24 of 1997.

Civil Court not to have Jurisdiction.

53. No civil court have jurisdiction to entertain any suit or proceedings in respect of any matter dealt with under the provisions of this Act.

CHAPTER VIII

Offences and Penalties

Punishment for offences related to personal data.

54. Whoever, except in compliance with the provisions of this Act, collects, stores, receives, processes, publishes or otherwise handles personal data shall be punishable with a term of imprisonment for a term which may extend up to five years and fine which may extend up to rupees fifty thousand for each day of unlawful access to the personal data:

Provided that where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly.

Punishment for offences related to sensitive personal data.

55. Whoever, except in compliance with the provisions of this Act, collects, stores, receives, processes, publishes or otherwise handles sensitive personal data shall be punishable with a term of imprisonment which may extend up to ten years and fine which may extend up to rupees one lakh for each day of unlawful access to the personal data and shall also be required to provide adequate compensation to the person whose sensitive personal data has been breached to be determined by the Authority in such manner as may be prescribed.

Breach of confidentiality and security in certain cases.

56. Whoever breaches confidentiality or compromises security of any personal data being collected as a part of surveillance authorised under this Act shall be liable to be punished with a term of imprisonment which may extend up to ten years and/or fine which may extend up to rupees fifty thousand for each day of said breach.

Compensation in case of harassment and profiling.

57. Whoever has been victim of profiling and harassment, whether physical or financial under section 42 shall be entitled to adequate compensation for financial loss and mental trauma in such manner as may be prescribed.

Penalty for contravention of directions.

58. Any wilful non-compliance of a direction or order of the Bench shall be punishable with imprisonment for a term which may extend upto six month and fine which may extend upto rupees fifty thousand for each day of said breach.

Cognizance.

2 of 1974.

59. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offences under this chapter shall be treated as cognizable.

CHAPTER IX

MISCELLANEOUS

Protection of action taken in good faith.

60. No suit or other legal proceeding shall lie against the Central Government, State Government, Chairperson or Member of the Authority, or any person acting under the direction either of the Central Government, State Government, Chairperson or Member of the Authority, as the case may be, in respect of anything which is in good faith done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.

Power to remove difficulties.

61. If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions, not inconsistent with the provisions of this Act, as appears to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of a period of three years from the commencement of this Act.

Overriding effect.

24 of 1997.
21 of 2000.

62. The provisions of this Act shall have overriding effect over the Telecom Regulatory Authority Act, 1997 the Information Technology Act, 2000 or any other legislation pertaining to collection, processing, interception and monitoring of personal data.

Power to make rules.

63. (*1*) The Central Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Act.

(*2*) Every rule made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or both the Houses agree that the rule should not be made, the rule shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule.

SCHEDULE I

[*See* Section 3(2)]

EXCEPTIONS

This Act shall not apply to collection or processing of data which falls within the following categories—

1. purely for personal reasons or pertaining to household activities;

2. of a deceased person;

3. eligible to be disclosed under the Right to Information Act, 2005; and

4. that is anonymised and cannot be used to identify the natural person.

SCHEDULE II

[*See* section 3]

PRIVACY NOTICE

Any privacy notice published under this Act must contain the following ingredients—

(*a*) What personal data or information is being collected;

(*b*) the purposes of the processing;

(*c*) the categories of personal data concerned;

(*d*) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations along with the safeguards thereof;

(*e*) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(*f*) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(*g*) the right to lodge a complaint with the competent authority;

(*h*) where the personal data are not collected from person, any available information as to their source.

(*i*) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the person.

STATEMENT OF OBJECTS AND REASONS

While right to life and personal liberty are granted under article 21 of the Constitution of India, our jurisprudence, judicial pronouncements and case laws have extended it to encompass *inter alia*, a life of dignity. However, there is no express statutory grant of right to privacy.

The Hon'ble Supreme Court has recognised the right to privacy in a limited and reasonable manner with the landmark case of *Kharak Singh v. The State of U.P.* It has further expounded on the principle and safeguards thereof in various landmark cases such as *PUCL v. Union of India* and *Selvi v. Union of India*, delineating the extent of the right to privacy in communications and the right to withhold consent to certain privacy violations, respectively.

With the increased proliferation of technology in daily lives, it is becoming increasingly important for us to recognise and implement a meaningful right to privacy as also recognised by the Special Rapporteur on the Right to Privacy, Office of the High Commissioner for Human Rights. Further, India has globally, as a party to the Universal Declaration of Human Rights (UDHR), and the International Covenant for Civil and Political Rights (ICCPR), acknowledged the right to privacy as an universal human right under Article 12 of the UDHR and Article 17 of the ICCPR.

On one hand, there is significant success of Aadhaar, which is the largest biometric database in the world, as a means to implement social welfare schemes and serves as a tool for financial inclusion. On the other hand, there is reasonable apprehension as to the security of the information contained in the database and during any information transmission as a part thereof.

Today, personal data is being collected and processed at a much larger scale that is not limited to AADHAAR; every application and website we use collects and processes our personal data. Our personal data is vulnerable to any non-State actor, private entity around the globe with the technological know-how to access and process this data unlawfully. It may be utilised by Non-State Actors to target Indian citizens through cyber-attacks for financial gains as well as to profile the interests of any person. Ready availability and accessibility of personal data can also assist terror groups or religiously extreme groups in profiling, propagating extremist ideology and preying on young, poor and destitute.

The present Bill is an effort to avoid situations like a country-wide hack like in the case of Estonia in 2007 and the recent global ransomware attack `WannaCry' in 2017. Globally, data is being considered the new oil and in the coming years, our international trade and economic relations will depend on the health and bargaining power of our data economy. Hence it is timely to address the issue on data protection and protect the privacy of all persons. It intends to provide rights of persons *vis-a-vis* their own information, as well as procedures for data collection, data processing, reasonable and targeted surveillance, and means of redress in case of breaches and violations.

In light of this, while the collection and processing of data is important, there is an overwhelming need to secure personal data and ensure better security by creating a statutory obligation to safeguard data and individuals. To that effect, this Bill seeks to establish *Inter alia*, a balance between rights of individuals and legitimate intervention by the State.

The Bill seeks to codify and safeguard the right to privacy for all juristic persons in the digital age, balanced with the need for data protection in the interests of national security.

Hence this Bill.

NEW DELHI;
April 7, 2017

BAIJAYANT PANDA

FINANCIAL MEMORANDUM

Clause 34 of the Bill provides for appointment of Data Protection Officer. Clause 44 provides for establishment of the Data Privacy Authority for carrying out the purposes of this Act. Clause 45 provides for the appointment of a Chairperson and other members to the Authority. Clause 46 provides for constitution of Benches by the Authority. The Bill, therefore, if enacted would involve expenditure from the Consolidated Fund of India. It is estimated that a sum of about rupees ten crores would involve as recurring expenditure per annum from the Consolidated Fund of India.

A non-recurring expenditure of about rupees fifty crores is also likely to be involved out of the Consolidated Fund of India.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 63 of the Bill empowers the Central Government to make rules for carrying out the purposes of the Act. As the rules will relate to matters of detail only, the delegation of legislative power is of a normal character.

LOK SABHA

———

A

BILL

to codify and safeguard the right to privacy in the digital age and constitute a Data Privacy Authority to protect personal data and for matters connected therewith.

———

(*Shri Baijayant Panda, M.P.*)

GMGIPMRND—889LS(S3)—10.07.2017.