As introduced in Lok Sabha

Bill No. 161 of 2017

THE DATA PRIVACY AND PROTECTION BILL, 2017

By

Dr. Shashi Tharoor, M.P.

A

BILL

to establish an effective regime to protect the right to privacy of data all natural person; to set out conditions of surveillance and interception of communications of natural persons; and to constitute a Privacy Commission and for matters connected therewith or incidental thereto.

WHEREAS the right to privacy is an inalienable right of all persons;

AND WHEREAS the need to protect privacy has increased in the digital age with the emergence of big data analytics;

AND WHEREAS the delivery of goods and provision of services requires the collection, storage, processing and disclosure including international transfers of personal data;

AND WHEREAS good governance requires that all interceptions of communications and surveillance must be conducted in a systematic and transparent manner subservient to the rule of law;

AND WHEREAS it is necessary to harmonise any conflicting interests and competing legislations;

NOW, THEREFORE, it is expedient to provide for an enforceable means to protect the privacy of persons;

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 extends to the whole of India and, save as otherwise provided in this Act, it shall also apply to any offence or contravention hereunder 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.

Definitions.

2. (*1*) In this Act unless the context otherwise requires, —

(*a*) "anonymise" means, in relation to personal data, the encryption or removal of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify a natural person or data subject;

(*b*) "appropriate government" means, in relation to the Central Government or a Union territory Administration, the Central Government; in relation to a State Government, that Government of that State; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly:

(*i*) by the Central Government or a Union Territory Administration, the Central Government;

(ii) by a State Government, the Government of that State;

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

(*d*) "authorised officer" means 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 the provisions of this Act;

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

(*f*) "Chief Privacy Commissioner" and "Privacy Commissioner" mean the Chief Privacy Commissioner and Privacy Commissioner, respectively appointed under section 33;

(*g*) "collect", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a data controller, police force, armed force, intelligence organisation, public authority, company, person, State or other entity (natural or otherwise) obtaining, or coming into the knowledge or possession of, any personal data of another person;

(*h*) "communication" means words, signs, gestures, 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, and the meta data in relation whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

(*i*) "competent organisation" means an organisation or public authority listed under Schedule to this Act;

(*j*) "consent" means an unambiguous indication of a data subject's agreement to the collection, processing, use or dissemination of personal data relating to him or her.

(*k*) "data controller" means a person who, either solely, or jointly or in combination with other persons, determines the purposes for which and the manner in which any personal data is processed;

(*l*) "data processor" means a person who processes any personal data on behalf of a data controller;

(*m*) "data subject" means a natural person who is the subject of personal data;

(*n*) "deoxyribonucleic acid data" means all data, of whatever type, concerning the characteristics of a natural person that are inherited or acquired during early prenatal development;

(*o*) "destroy", with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data;

(*p*) "disclose", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person coming into the knowledge or possession of any personal data of another person;

(*q*) "intelligence organisation" means an intelligence organisation under the Intelligence Organisations (Restriction of Rights) Act, 1985 and includes the National Investigation Agency constituted under sub-section (1) of section 3 of the National Investigation Agency Act, 2008 and the Central Bureau of Investigation constituted under the Delhi Special Police Establishment Act, 1946;

(*r*) "interception" or "intercept" means any activity intended to capture, read, listen to or understand the communication of a person;

(*s*) "officer-in-charge of a police station" shall have the meaning ascribed to it under clause (*o*) of section 2 of the Code of Criminal Procedure, 1973

(*t*) "person" means and includes a natural person, a company, a firm, an association of persons or a body of individuals, whether incorporated or not;

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

Provided that the term "personal data" shall not include data which is a matter of public record except details of victims in cases of sexual assault, kidnapping or abduction.

(*v*) "police force" means—

(*i*) anybody raised or constituted by the appropriate government for the preservation of law and order and enforcement of laws related to customs, revenue, foreign exchange, excise, income tax and narcotics;

(*ii*) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Police Act, 1861, the Central Reserve Police Force Act, 1949, the Border Security Force Act, 1968, the Indo-Tibetan Border Police Force Act, 1992, the Sashastra Seema Bal Act, 2007, the Central Industrial Security

Force Act, 1968, the Railway Protection Force Act, 1957 and the National Security Guard Act, 1986; or

(*iii*) the bodies raised or constituted pursuant to or in connection with, or presently governed by, the Delhi Special Police Establishment Act, 1946, the Income Tax Act, 1961, the National Investigation Agency Act, 2008 and the Central Vigilance Commission Act, 2003; or

(*iv*) any police forces raised or constituted by the States, armed or otherwise;

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

(*x*) "Privacy Commission" means the Privacy Commission constituted under sub-section (*1*) of section 33;

(*y*) "Privacy Officer" means the Privacy Officer designated under sub-section (*3*) of section 22 and sub-sections (*3*) and (*4*) of section 30.

(*z*) "process", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data of another person, whether or not by automated means including, but not restricted to, organisation, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction;

(*za*) "public authority" shall have the meaning ascribed to it under clause (h) of section 2 of the Right to Information Act, 2005;

(*zb*) "receive", with its grammatical variations and cognate expressions, means, in relation to personal data, to come into the knowledge or possession of any personal data of another person;

(*zc*) "sensitive personal data" means personal data or metadata including—

(*i*) biometric data;

(*ii*) deoxyribonucleic acid data;

(*iii*) sexual preferences and practices;

(*iv*) medical history and health;

(*v*) political affiliation;

(*vi*) ethnicity, religion, race or caste; and

(*vii*) financial and credit information, including financial history and transactions.

(*zd*) "store", with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data of another person; and

(*ze*) "surveillance" means any activity, directly or indirectly intended to watch, monitor, record or collect, or to enhance the ability to watch, record or collect, any information, images, signals, data, movement, behaviour or actions, of a person, a group of persons, a place or an object, for the purpose of obtaining information of a person, but does not include collection of personal data under sections 7 and 8 of this Act.

(*2*) All other expressions used herein shall have the meanings assigned to them under the General Clauses Act, 1897 or the Code of Criminal Procedure, 1973, as the case may be.

Principles applicable to protecting privacy.

3. In exercising the powers conferred by this Act, regard shall be had to the following considerations, namely: —

(*a*) that personal data with its attributes belongs solely to the person to whom it pertains;

(*b*) that personal data is required by Governments and commercial service providers and others to enable good governance and the delivery of goods and provision of services without undue delay which may be provided by a meaningful, revocable notice and consent framework;

(*c*) that the right to privacy is recognised as a fundamental human right by various international treaties to which India is a party;

(*d*) that intrusions into privacy need always be measured by principles of necessity and proportionality;

(*e*) that the right to privacy is a fundamental right essential to the maintenance of a democratic society; and

(*f*) that privacy must be upheld by a competent authority that is independent, impartial, well resourced and free from unwarranted influence.

CHAPTER II

RIGHT TO PRIVACY

Right to privacy.

4. (*1*) Without prejudice to the generality of the provisions contained herein, all natural persons shall have a right to privacy which shall be implemented subject to provisions of section 3.

(*2*) For the purpose of sub-section (*1*) no person shall collect, store, process, disclose or otherwise handle any personal data of a natural person, intercept any communication of another person, or carry out surveillance of another person except in accordance with the provisions of this Act.

Exemptions.

5. Nothing in this Act shall apply to—

(*a*) the collection, storage or processing by a person of their own personal data for personal or family use; or

(*b*) surveillance by a resident of their own residential property.

CHAPTER III

PROTECTION OF PERSONAL DATA

Effective consent from a data subject.

6. A data subject may be said to have given effective consent only when it is—

(*1*) free, in the terms of section 14 of the Indian Contract Act, 1872;

(*2*) obtained prior to all data collection, except in the cases expressly excluded by section 8;

(*3*) voluntarily given through an express and affirmative act and is recorded in writing:

Provided that effective consent shall only be said to have been obtained where:

(*i*) a conspicuous means for its withdrawal is made available to the data subject; and

(*ii*) the means for its withdrawal may be employed with the same ease as the means by which it was obtained.

(*4*) obtained after the data subject has been duly informed, in language that a reasonable person may comprehend, of the matters enumerated in sub-section (*3*) of section 7 or sub-section (*3*) of section 13 as the case may be, and:

Provided that, in case of any dispute, ambiguities in the terms of the notice and of any privacy policies that apply will be resolved in favour of the data subject;

(*5*) specific and limited as to the purpose and duration.

Explanation 1.—For the purposes of this section consent shall be deemed to be limited only if it is obtained in respect of the purposes and duration strictly necessary to provide the product or service in relation to which personal data is sought to be collected, processed or disclosed;

Explanation 2.—When the purposes for which personal data was collected are materially altered or expanded subsequent to its collection, consent shall be deemed to be specific only if it is obtained afresh in respect of that alteration or expansion—

(*i*) after duly informing the data subject of the alteration or expansion in purpose, and

(*ii*) prior to any use of that data for the expanded purposes.

Collection of personal data.

7. (*1*) No person, including a data controller and data processor, shall collect any personal data without obtaining the effective consent of the data subject to whom it pertains.

(*2*) Subject to sub-section (*1*), no person shall collect any personal data that is not necessary for the achievement of a purpose that is connected to a stated function of the person seeking its collection.

(*3*) A person seeking to collect any personal data shall, prior to its collection and as notified by the Privacy Commission, inform the data subject free of any charges, direct or indirect, to whom it pertains of the following details in respect of their personal data, namely—

(*a*) when it shall be collected;

(*b*) its content and nature;

(*c*) the purpose of its collection;

(*d*) the purpose and manner in which it shall be used;

(*e*) the persons to whom it shall be made available;

(*f*) the duration for which it shall be stored;

(*g*) the manner in which it may be accessed, checked and modified;

(*h*) the security practices and other safeguards, if any, to which it shall be subject;

(*i*) the privacy policies and other policies, if any, that shall protect it;

(*j*) whether, and the conditions and procedure upon which, it may be disclosed to others;

(*k*) the time and manner in which it shall be destroyed, or the criteria used to determine that time period;

(*l*) the procedure for recourse in case of any grievance in relation to it; and

(*m*) the identity and contact details of the data collector and data processor.

(*4*) The personal data collected in pursuance of a grant of consent by the data subject to whom it pertains shall, if that consent is subsequently withdrawn for any reason, be destroyed forthwith:

Provided that the person who collected the personal data in respect of which consent is subsequently withdrawn may, only if the personal data is necessary for the delivery of any good or the provision of any service, or the fulfillment of a lawful

contract, not deliver that good or deny that service or fulfil that contract to the data subject who withdrew the grant of consent easily and at any point during the duration of a service.

Collection of personal data without prior consent.

8. Personal data may be collected without the prior consent of the data subject if it is—

(*a*) necessary for the provision of an emergency medical service to the data subject;

(*b*) required for the establishment of the identity of the data subject and the collection is authorised by a law in this regard; and

(*c*) necessary to prevent, investigate or prosecute a cognisable offence.

Storage and destruction of personal data.

9. (*1*) No person, including a data controller and a data processor, shall store any personal data 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 data subject to whom it pertains grants their effective 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 adduced for an evidentiary purpose in a legal proceeding; or

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

Provided that only such 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:

Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

Processing of personal data.

10. (*1*) No person shall process any personal data that is not necessary for the achievement of the purpose for which it was collected or received.

(*2*) Save as provided in sub-section (*3*), no personal data shall be processed for any purpose other than the purpose for which it was collected or received.

(*3*) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if the data subject grants their effective consent to such processing and only that amount of personal data that is necessary to achieve the other purpose is processed.

(*4*) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if —

(*a*) the data subject grants his/her effective consent to the processing and only that amount of personal data that is necessary to achieve the other purpose is processed;

(*b*) it is necessary to perform a contractual duty to the data subject;

(*c*) it is necessary to prevent a reasonable threat to security of the State or public order; or

(d) it is necessary to prevent, investigate or prosecute a cognisable offence.

Security of personal data and duty of confidentiality.

11. (*1*) No person shall collect, receive, store, process or otherwise handle any personal data without implementing measures, including, but not restricted to, technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, integrity and safety, including from theft, loss, damage or destruction.

(*2*) Any person who collects, receives, stores, processes or otherwise handles any personal data shall be subject to a duty of confidentiality and secrecy in respect of it.

(*3*) The data controllers and data processors shall be subject to a duty of confidentiality and secrecy in respect of personal data in their possession or control.

(*4*) Without prejudice to the provisions of this section, any person who collects, receives, stores, processes or otherwise handles any personal data shall, if its confidentiality, secrecy, integrity or safety is violated by theft, loss, negligence, damage or destruction, or as a result of any collection, processing or disclosure contrary to the provisions of this Act, or for any other reason whatsoever, as soon as he or she becomes aware of such violation, notify the person to whom it pertains, the Privacy Commission and any other agencies whom the Central Government notifies for this purpose, in such form and manner as may be prescribed, forthwith. Further, any persons, who collects, receives, stores, processes, or otherwise handles any personal data shall report all breaches of provisions of this Chapter III to the Privacy Commission, that are brought to its notice, or are reasonably expected to be known to such persons.

Transfer of personal data for processing.

12. (*1*) Subject to the provisions of this section, personal data that has been collected in conformity with this Act may be transferred by a data controller for to a data processor, whether located in India or otherwise, if the transfer is pursuant to an agreement that explicitly binds the data processor to same or stronger measures in respect of the storage, processing, destruction, disclosure and other handling of the personal data as are contained in this Act.

(*2*) No data processor shall process any personal data transferred under this section except to achieve the purpose for which it was collected.

(*3*) A data controller that transfers personal data under this section shall remain liable to the data subject for the actions of the data processor.

Disclosure of personal data.

13. (*1*) Save as provided in this section, no person shall disclose, or otherwise cause any other person to receive, the content or nature of any personal data, including any other details in respect thereof, except to the person to whom it pertains.

(*2*) No person shall disclose any personal data without obtaining the prior effective consent of the data subject and such effective consent may be obtained in any manner, and through any medium, but shall not be obtained as a result of a threat, duress, denial of service or coercion.

(*3*) For the purpose of sub-section (*2*), a person seeking to disclose any personal data shall, prior to its disclosure, inform the data subject of the following details in respect of their personal data, namely: —

(*a*) when it shall be disclosed;

(*b*) the purpose of its disclosure;

(*c*) the security practices and other safeguards, if any, to which it shall be subject to;

(*d*) the privacy policies and other policies, if any, that shall protect it; and

(*e*) the procedure for recourse in case of any grievance in relation to it.

(*4*) Notwithstanding anything contained in this section, any person who collects, receives, stores, processes or otherwise handles any personal data may disclose it to a person other than the data subject, whether located in India or otherwise, for the purpose only of processing it to achieve the purpose for which it was collected if such a disclosure is pursuant to an agreement that explicitly binds the person receiving it to same or stronger measures in respect of its storage, processing, destruction, disclosure or other handling as are contained in this Act.

Quality and accuracy of personal data.

14. (*1*) Any person who collects, receives, stores, processes or otherwise handles any personal data shall, to the extent possible, ensure that it is accurate and, where necessary, is kept up to date.

(*2*) No person who collects, receives, stores, processes or otherwise handles any personal data shall deny, to the data subject, the opportunity to review and obtain a copy of such data and, where necessary, rectify anything that is inaccurate or not up to date.

(*3*) Any person to whom any personal data collected, received, stored, processed or otherwise handled under this Act pertains may, if it is not necessary to achieve the purpose of its collection, reception, storage, processing or other handling, demand its destruction, and the person so collecting, receiving, storing, processing or otherwise handling that personal data shall destroy it forthwith.

Special provisions for sensitive personal data.

15. Notwithstanding anything contained in this Act and the provisions of any other law for the time being in force—

(*a*) no person shall collect sensitive personal data without explicit effective consent from the data subject;

(*b*) no person shall store sensitive personal data 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;

(*c*) no person shall process sensitive personal data for a purpose other than the purpose for which it was collected or received; and

(*d*) no person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any sensitive personal data, including any other details in respect thereof, except the data subject.

Special provisions for intelligence organisations.

16. (*1*) Notwithstanding anything contained in this Act, the provisions of sections 6, 7, 8, sub-section (*4*) of section 10 and section 11 shall not apply in respect of an intelligence organisation.

(*2*) Any intelligence organisation seeking to collect any personal data shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(*3*) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the collection of the personal data is necessary to prevent a reasonable threat to security of the state or public order, or prevent, investigate or prosecute a cognisable offence, order the collection of the personal data by recording reasons in writing within a period of fourteen days from the receipt of an application under sub-section (*2*).

(*4*) Notwithstanding anything contained in sub-section (*2*) and subsection (*3*), if the Central Government is satisfied that a serious threat to the security of the State or public order exists, it may, for reasons to be recorded in writing, which shall include the reason for not getting an order under sub-section (*3*), order the collection of any personal data.

(*5*) Before the expiry of a period of seven days from the date of an order for collection of personal data made under sub-section (*4*), the intelligence organisation that collected the personal data shall notify the Chief Privacy Commissioner of the fact of such collection, the name and address of the person to whom the personal data pertains and shall furnish a copy of the order of the Central Government authorising the collection of the personal data.

(*6*) No intelligence organisation shall process or store any personal data without implementing measures to secure that the number of persons within that intelligence organisation to whom it is made available, and the extent to which it is copied, is limited to the minimum that is necessary to fulfill the purpose for which it is processed or stored, as the case may be.

(*7*) Any intelligence organisation that processes or stores personal data shall, before the expiry of a period of seven days from the date of the processing or storage, as the case may be, notify the Chief Privacy Commissioner of the fact of such processing or storage and the name and address of the person to whom the personal data pertains.

(*8*) Any intelligence organisation that processes or stores personal data shall have to comply with the provisions of section 10 with respect to such data.

CHAPTER IV

INTERCEPTION OF COMMUNICATIONS

Bar against interception of communications.

17. (*1*) Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall intercept, or cause to be intercepted, any communication of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(*2*) No interception of any communication shall be ordered or carried out that is not necessary to achieve the purpose for which the interception is sought.

Prior authorisation by the Chief Privacy Commissioner.

18. (*1*) Any authorised officer seeking to intercept any communication of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(*2*) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, if he is satisfied that the interception is necessary to prevent a reasonable threat to security of the state or public order, or prevent, investigate or prosecute a cognisable offence, order the interception of communications by recording reasons in writing within a period of fourteen days from the receipt of an application under sub-section (*1*).

(*3*) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall prior to issuing an order for interception of any communication, satisfy himself that all other lawful means to acquire the information sought to be intercepted have been exhausted and that the proposed interception is reasonable, proportionate and not excessive.

(*4*) Any interception of any communication ordered, authorised or carried out prior to the commencement of this Act shall, immediately upon the constitution of the Privacy Commission, be reported to the Chief Privacy Commissioner.

Authorisation by Home Secretary in emergent circumstances.

19. (*1*) Notwithstanding anything contained in section 17, if the Home Secretary of the appropriate government is satisfied that an imminent serious threat to the security of the State or public order exists, he may, for reasons to be recorded in writing, order the interception of any communication.

(*2*) No order for interception of any communication made under this section shall be valid upon the expiry of a period of seven days from the date of the order.

(*3*) Before the expiry of a period of seven days from the date of an order for interception made under this section, the person who carried out the interception of communication shall notify the Chief Privacy Commissioner of the fact of such interception, the name and address of the person whose communication is being intercepted, and the duration of the interception

and, furthermore, shall furnish a copy of the order of the Home Secretary authorising the interception.

Duration of interception.

20. (*1*) An order for interception of any communication shall specify the period of its validity and, upon the expiry of the validity of the order, all interception carried out in relation to that order shall cease forthwith:

Provided that no order for interception of any communication shall be valid upon the expiry of a period of sixty days from the date of such order.

(*2*) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for interception of any communication if he is satisfied that the conditions upon which the original order was issued continue to exist.

Duty to inform the person concerned.

21. (*1*) Subject to sub-section (*2*), before the expiry of a period of sixty days from the conclusion of any interception of communication ordered or carried out under this Act, the authorised officer who carried out the interception of communication shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of the Chief Privacy Commissioner, each person whose communication was intercepted of the fact of such interception and duration thereof.

(*2*) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) may reasonably present a reasonable threat to the security of the state or public order, or adversely affect the prevention, investigation or prosecution of a cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order that the person whose communication was intercepted not be notified of the fact of such interception or the duration thereof:

Provided any orders passed preventing disclosure of interception under section (*2*) shall not operate in infinity and shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on whose cessation the duty to inform under sub-section (*1*) shall operate.

Security and duty of confidentiality and secrecy.

22. (*1*) No person shall intercept any communication of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of an interception of communication, including from theft, negligence, loss or unauthorised disclosure.

(*2*) Any person who carries out any interception of any communication, or who obtains any information, including personal data, as a result of an interception of communication, shall be subject to a duty of confidentiality and secrecy in respect of it.

(*3*) Every competent organisation shall, before the expiry of a period of one hundred days from the date of enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for administration of all interceptions of communications carried out by that competent organisation.

Disclosure of intercepted communications.

23. (*1*) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of an interception of any communication including the fact that the interception of communication was carried out.

(*2*) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of an interception of any communication is necessary to prevent a reasonable threat to the security of the state or public order, or prevent, investigate or prosecute a cognisable offence, an authorised officer may disclose the information, including personal data, obtained as a result of the

interception of any communication to any authorised officer of any other competent organization:

Provided that no authorised officer shall disclose any information, including personal data, obtained as a result of the interception of any communication that is not necessary to achieve the purpose for which the disclosure is sought.

Storage of intercepted communications.

24. (*1*) Subject to sub-section (*2*), no person shall store any information, including personal data, obtained as a result of an interception of any communication for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.

(*2*) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognizable offence, for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of an interception of any communication may be stored for a period longer than one hundred and eighty days from the date on which the last order for interception of the communication to which the obtained information pertains expired.

(*3*) Any data obtained as a result of interception of any communication shall be stored in a manner that complies with the provisions of section 9 with respect to such data.

CHAPTER V

SURVEILLANCE

Bar against surveillance.

25. Notwithstanding anything contained in any other law for the time being in force, but save as provided in this chapter, no person shall order or carry out, or cause or assist the ordering or carrying out of, any surveillance of another person:

Provided that there shall be an absolute bar to the subjection of persons to indiscriminate monitoring through any methods of mass or bulk surveillance given that it is neither necessary or proportionate to any stated purpose including but not limited to the security of state, interests of public order or to prevent, investigate or prosecute a commission of a cognizable offence.

Surveillance by the State.

26. (*1*) No member of a police force, armed force, intelligence organisation, public authority or the State shall order or carry out, or cause to be ordered or carried out, any surveillance of another person save in pursuance of an order by the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(*2*) No surveillance shall be ordered or carried out that is not necessary to achieve the purpose for which the surveillance is sought.

(*3*) Any authorised officer seeking to carry out any surveillance of another person shall prefer an application, in such form and manner as may be prescribed, to the Chief Privacy Commissioner or any other person authorised by him in this behalf.

(*4*) The Chief Privacy Commissioner, or any other person authorised by him this behalf, may, if he is satisfied that the surveillance is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognizable offence, for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.

(*5*) Prior to issuing an order for surveillance, the Chief Privacy Commissioner, or any other person authorised by him in this behalf, shall satisfy himself that all other lawful means to acquire the information sought to be obtained as a result of the proposed surveillance have been exhausted and that the proposed surveillance is reasonable, proportionate and not excessive.

Surveillance by private persons or entities.

27. (*1*) Notwithstanding anything contained in any other law for the time being in force, and without prejudice to the provisions of section 25, no person who is not a member of a police force, armed force, intelligence organisation, public authority or the State shall carry out, or cause to be carried out, any surveillance in any public place or in any property or premises that is not in his possession.

(*2*) Without prejudice to sub-section (*1*), any person who carries out any surveillance under this section shall be subject to a duty to inform, in such manner as may be prescribed, members of the public of such surveillance.

Duration of surveillance.

28. (*1*) An order for surveillance shall specify the period of its validity and, upon the expiry of the validity of the order, all surveillance carried out in relation to that order shall cease forthwith:

Provided that no order for surveillance shall be valid upon the expiry of a period of sixty days from the date of the order.

(*2*) The Chief Privacy Commissioner, or any other person authorised by him in this behalf, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed, renew any order for surveillance if he is satisfied that the conditions upon which the original order was issued continue to exist.

Duty to inform the person concerned.

29. (*1*) Subject to sub-section (*2*), before the expiry of a period of sixty days from the conclusion of any surveillance ordered or carried out under this Act, the authorised officer who carried out the surveillance shall, in writing in such form and manner as may be prescribed, notify, with reference to the relevant order of the Chief Privacy Commissioner, each person in respect of whom surveillance was carried out of the fact of such surveillance and duration thereof.

(*2*) The Chief Privacy Commissioner may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (*1*) may present a reasonable threat to the security of the State or public order, or adversely affect the prevention, investigation or prosecution of a cognizable offence, for reasons to be recorded in writing addressed to the authorised officer, order that the person not be notified of the fact of such surveillance or the duration thereof:

Provided that any order passed which prevent disclosure of surveillance under Sub-section (2) shall not operate in infinity and the Chief Privacy Commissioner shall record reasons in writing with the period till when the reasonable threat is anticipated to extend, on whose cessation the duty to inform under sub-section (1) shall operate.

Security and duty of confidentiality and secrecy.

30. (*1*) No person shall carry out any surveillance of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of surveillance, including from theft, loss or unauthorised disclosure.

(*2*) Any person who carries out any surveillance, or who obtains any information, including personal data, as a result of surveillance, shall be subject to a duty of confidentiality and secrecy in respect of it.

(*3*) Every police force, armed force, intelligence organisation, public authority or State shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all surveillance carried out:

Provided that a public authority that does not order or carry out surveillance shall not be required to designate any Privacy Officers under this sub-section.

(*4*) Every person who is not a member of a police force, armed force, intelligence organisation, public authority or State and who seeks to carry out any surveillance shall, at least seven days before the surveillance is first carried out, designate or appoint as many

persons as it deems fit as Privacy Officers who shall be responsible for all surveillance carried out:

Provided that where surveillance is carried out by a single person, that person shall be deemed to be a Privacy Officer.

Disclosure of surveillance.

31. (*1*) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of any surveillance including the fact that the surveillance was carried out.

(*2*) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of surveillance is necessary to prevent a reasonable threat to the security of the State or public order, or prevent, investigate or prosecute a cognizable offence, that information, including personal data, obtained as a result of surveillance may be disclosed to a police force, armed force, intelligence organisation, public authority or State only:

Provided that no person shall disclose any information, including personal data, obtained as a result of surveillance that is not necessary to achieve the purpose for which the disclosure is sought.

Storage of surveillance data.

32. (*1*) Subject to sub-section (*2*), no person shall store any information, including personal data, obtained as a result of surveillance for a period longer than one hundred and eighty days from the date on which the surveillance to which the obtained information pertains ceased.

(*2*) The Chief Privacy Commissioner may, on an application made in such form and manner as may be prescribed, if he is satisfied that it is necessary to prevent a reasonable threat to the security of the state or public order, or to prevent, investigate or prosecute a cognizable offence, for reasons to be recorded in writing, order that any information, including personal data, obtained as a result of surveillance may be stored for a period longer than one hundred and eighty days from the date on which the last order for surveillance to which the obtained information pertains expired.

(*3*) Any data obtained as a result of surveillance shall be stored in a manner that complies with the provisions of section 9 with respect to such data.

CHAPTER VI

THE PRIVACY COMMISSION

Constitution of the Privacy Commission.

33. (*1*) The Central Government shall, by notification, constitute, with effect from such date as may be specified therein, a body to be called the Privacy Commission consisting of a Chief Privacy Commissioner and not more than six other Privacy Commissioners, to be appointed by the President, by warrant under its hand and seal, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon them by or under this Act.

(*2*) The Chief Privacy Commissioner shall be a person who has been a Judge of the Supreme Court of India.

(*3*) One Privacy Commissioner shall be a person who is or has been a Judge of a High Court.

(*4*) One Privacy Commissioner shall be a person of ability, integrity and standing who has a special knowledge of, and professional experience of not less than ten years in privacy law and policy.

(*5*) The other Privacy Commissioners shall be persons with technical expertise and knowledge in the fields of data collection and storage practices, or data protection and ethics, or big data analytics and technologies or information technology while one Privacy

Commissioner should be an ordinary citizen representing the interests of the public who are consumers of data.

(*6*) The headquarters of the Privacy Commission shall be at New Delhi:

Provided that the Central Government shall, in consultation with the Chief Privacy Commissioners may establish its offices at such other places at it deems fit.

(*7*) The office of the Privacy Commission shall be a body corporate by the name of aforesaid, autonomous, independent, and free from external interference and shall be the said name, sue or be sued.

(*8*)The office of the Privacy Commission shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers:

Provided that such powers shall be subject to audit by the Comptroller and Auditor General of India.

(*9*) The Central Government shall issue a public advertisement inviting applications to fill all vacancies in the Privacy Commission.

(*10*) For the purpose of filling vacancies under sub-section (8) the Privacy Commissioner shall constitute a selection committee which shall consist of the Chief Justice of India, the Law Minister, the Leader of the Opposition from the House of the People or of the single largest Opposition party being one with the greatest numerical strength in the House of the People, one eminent person representing the private sector and one eminent person representing the civil society to be nominated by the Central Government in such manner as may be prescribed.

(*11*) Every proceeding of the selection committee shall constitute as a public record.

Explanation. For the purpose of this section, the term "Civil society" shall mean the aggregate of non-Governmental and non-profit organisations that perform activities for the general upliftment and interests of the people in the field of privacy and is independent of government funding, interference or influence.

Term of office, conditions of service, etc. of Chief Privacy Commissioner and Privacy Commissioners.

34. (*1*) The President shall before appointing any person as the Chief Privacy Commissioner or Privacy Commissioner, as the case may be, satisfy himself that the person does not, and shall not, have any such financial or other interest as is likely to affect prejudicially their functions as such Chief Privacy Commissioner or Privacy Commissioner as the case may be.

(*2*) The Chief Privacy Commissioner and every Privacy Commissioner shall hold office for such period, not exceeding five years, as may be specified by the President in the order of his appointment and be eligible for reappointment:

Provided that no person shall hold office as the Chief Privacy Commissioner or Privacy Commissioner for more than two terms;

Provided further that no person shall hold office as the Chief Privacy Commissioner or Privacy Commissioner after they have attained the age of seventy-five years.

(*3*) Notwithstanding anything contained in sub-section (2), the Chief Privacy Commissioner or any Privacy Commissioner may—

(*a*) by writing under his hand and addressed to the President resign his office at any time; or

(*b*) be removed from office in accordance with the provisions of section 35.

(*4*) A vacancy caused by the resignation or removal of the Chief Privacy Commissioner or Privacy Commissioner under sub-section (*3*) shall be filled by fresh appointment.

(*5*) In the event of the occurrence of a vacancy in the office of the Chief Privacy Commissioner, the President may, by notification, authorise in his behalf, one of the Privacy Commissioners as the Chief Privacy Commissioner till the date on which a new Chief Privacy Commissioner, appointed in accordance with the provisions of this Act, enters upon his office.

(*6*) When the Chief Privacy Commissioner is unable to discharge his functions owing to absence, illness or any other cause, such one of the Privacy Commissioners as the Chief Privacy Commissioner may authorise in writing in this behalf shall discharge the functions of the Chief Privacy Commissioner, till the date on which the Chief Privacy Commissioner resumes his duties.

(*7*) **The salaries and allowances payable to and the other terms and conditions of service of the Chief Privacy Commissioner and Privacy Commissioners shall be such as may be prescribed:**

Provided that neither the salary and allowances nor the other terms and conditions of service of the Chief Privacy Commissioner and any Privacy Commissioner shall be varied to their disadvantage after their appointment.

(*8*) The Chief Privacy Commissioner and Privacy Commissioners ceasing to hold office as such shall not hold any appointment under the Government of India or under the Government of any State for a period of five years from the date on which they cease to hold such office.

Removal of Chief Privacy Commissioner and Privacy Commissioners from office in certain circumstances.

35. (*1*) The President may remove from office the Chief Privacy Commissioner or any Privacy Commissioner, who —

(*a*) is adjudged an insolvent; or

(*b*) engages during his term of office in any paid employment outside the duties of his office; or

(*c*) is unfit to continue in office by reason of infirmity of mind or body; or

(*d*) is of unsound mind and stands so declared by a competent court; or

(*e*) is convicted for an offence which in the opinion of the President involves moral turpitude; or

(*f*) has acquired such financial or other interest as is likely to affect prejudicially his functions as a Chief Privacy Commissioner or Privacy Commissioner, or cause some conflict of interest including benefits directly or indirectly to relatives or family members, or

(*g*) has so abused his position as to render his continuance in offence prejudicial to the public interest.

(*2*) Notwithstanding anything contained in sub-section (*1*), neither the Chief Privacy Commissioner nor any Privacy Commissioner shall be removed from his office on the ground specified in clause (*f*) or clause (*g*) of that sub-section unless the Supreme Court on a reference being made to it in this behalf by the President, has on an inquiry held by it in accordance with such procedure as it may specify in this behalf, reported that the Chief Privacy Commissioner or Privacy Commissioner ought, on such grounds, to be removed.

Functions of the Privacy Commission.

36. (*1*) The Privacy Commission may, through decisions arrived at by a simple majority of its members present and voting as set out in Section 44(*1*) of this Act, authorise, review, investigate, make an inquiry, and/or monitor, *suo moto* or on a petition presented to it by any person or by someone acting on his behalf, the implementation and application of this Act and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

(*2*) Without prejudice to the generality of the foregoing provision, the Privacy Commission shall perform all or any of the following functions, namely—

(*a*) review the safeguards provided under this Act and under other laws for the time being in force for the protection of personal data and recommend measures for their effective implementation or amendment, as may be necessary from time to time;

(*b*) authorise, review, investigate, make an inquiry, and/or monitor any measures taken by any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity for the protection of privacy and take such further action is it deems fit;

(*c*) authorise, review, investigate, make an inquiry, and/or monitor any action, code, certification, policy or procedure of any competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to ensure compliance with this Act and any rules made hereunder;

(*d*) Investigate and direct data controllers and processors to do or cease to do any act in order to address activity which is in contravention of the provisions of this Act;

(*e*) formulate through public consultation with experts, other stakeholders, and the general public, norms for the effective protection of privacy by competent organisations, police forces, armed forces, intelligence organisations, public authorities, companies, persons or other entities;

(*f*) promote awareness and knowledge of personal data protection through any means necessary and to all stakeholders including providing information to any data subject regarding their rights under this Act as requested ;

(*g*) undertake and promote research in the field of protection of personal data and privacy;

(*h*) encourage the efforts of non-governmental organisations and institutions working in the field of personal data protection and privacy;

(*i*) publish periodic reports concerning the incidence of compliance including violations of this Act and data breaches as reported under sub-section (4) of section 11 of this Act, collection, processing, storage, disclosure and other handling of personal data, interception of communications and surveillance;

(*j*) hear and decide applications for interception and surveillance under Chapters IV and V of this Act;

(*k*) exercise its powers under section 28, to ensure the speedy and efficient redressal of all complaints whose cause of action arises from this Act; and

(*l*) such other functions as it may consider necessary for the protection of privacy, personal data, and enforcement of this Act.

(*3*) The Periodic Reports published by the Privacy Commission, stipulated in sub-section (*2*) of section 36, shall be tabled by the Central Government before the House of the People during the Parliamentary Session that succeeds the publication of such Periodic Report.

(*4*) The Chief Privacy Commissioner and the Privacy Commissioners shall appear before an *ad hoc* Committee, constituted by the Speaker of the House of the People and comprising of members from both the governing and the opposition parties from both houses of Parliament to be nominated by presiding officers of the House concerned, on an annual basis, in such manner as may be prescribed which shall,—

(*i*) review the functioning of the Privacy Commission, and may ask the Chief Privacy Commissioner and the Privacy Commissioners any questions in this regard; and

(ii) present periodic reports to both houses of Parliament in such manner as may be prescribed.

(*5*) Subject to the provisions of any rules prescribed in this behalf by the Central Government, the Privacy Commission shall have the power to review any decision, judgement, decree or order made by it.

(*6*) In the exercise of its functions under this Act, the Privacy Commission shall give such directions or pass such orders as are necessary for reasons to be recorded in writing.

Secretary, officers and other employees of the Privacy Commission.

37. (*1*) The Central Government shall appoint a Secretary to the Privacy Commission to exercise and perform, under the control of the Chief Privacy Commissioner such powers and duties as may be prescribed.

(*2*) The Central Government may provide the Privacy Commission with such other officers and employees as may be necessary for the efficient performance of the functions of the Privacy Commission.

(*3*) The salaries and allowances payable to and the conditions of service of the Secretary and other officers and employees of the Privacy Commission shall be such as may be prescribed.

Vacancies, etc. not to invalidate proceedings of the Privacy Commission.

38. No act or proceedings of the Privacy Commission shall be questioned on the ground merely of the existence of any vacancy or defect in the constitution of the Privacy Commission or any defect in the appointment of a person acting as the Chief Privacy Commissioner or Privacy Commissioner.

Chief Privacy Commissioner, Privacy Commissioners and employees of the Privacy Commission to be public servants.

39. The Chief Privacy Commissioner and Privacy Commissioners and other employees of the Privacy Commission shall be deemed to be a public servant within the meaning of section 21 of the Indian Penal Code, 1860.

Procedure to be followed by the Privacy Commission.

40. (*1*) Subject to the provisions of this Act, the Privacy Commission shall have powers to regulate —

(*a*) the procedure and conduct of its business; and

(*b*) the delegation to one or more Privacy Commissioners of such powers or functions as the Chief Privacy Commissioner may specify.

(*2*) In particular and without prejudice to the generality of the foregoing provisions, the powers of the Privacy Commission shall include the power to determine the extent to which persons interested or claiming to be interested in the subject-matter of any proceeding before it may be allowed to be present or to be heard, either by themselves or by their representatives or to cross-examine witnesses or otherwise take part in the proceedings:

Provided that any such procedure as may be prescribed or followed shall be guided by the principles of natural justice.

Power relating to inquiries.

41. (*1*) The Privacy Commission shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying suits in respect of the following matters, namely—

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

(*b*) the discovery and production of any document or other material object producible as evidence;

(*c*) the reception of evidence on affidavit;

(*d*) the requisitioning of any public record from any court or office;

(*e*) the issuing of any commission for the examination of witnesses; and

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

(*2*) The Privacy Commission shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Privacy Commission, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of sections 176 and 177 of the Indian Penal Code, 1860.

(*3*) The Privacy Commission or any Gazetted Officer, specially authorised in this behalf by the Privacy Commission may enter any building or place where the Privacy Commission has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973, in so far as it may be applicable.

(*4*) The Privacy Commission shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code, 1860 is committed in the view or presence of the Privacy Commission, the Privacy Commission may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973, forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under section 346 of the Code of Criminal Procedure, 1973.

Decisions of the Privacy Commission.

42. (*1*) The decisions of the Privacy Commission shall be taken by majority of the member present and voting and be binding and enforceable as a decree of a court as per the provisions of the Code of Civil Procedure, 1908.

(*2*) In its decisions, the Privacy Commission shall have the power to—

(*a*) require a competent organisation, police force, armed force, intelligence organisation, public authority, company, person or other entity to take such steps as may be necessary to secure compliance with the provisions of this Act;

(*b*) require a competent organisation, police force, armed force, intelligence organisation,public authority, company, person or other entity to compensate any person for any loss or detriment suffered; and

(*c*) impose any of the penalties provided under this Act.

Proceedings before the Privacy Commission to be judicial proceedings.

43. The Privacy Commission shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973, and every proceeding before the Privacy Commission shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 and for the purposes of section 196 of the Indian Penal Code, 1860.

Appeal.

44. No order passed under this Act shall be appealable except as provided therein and no civil court shall have jurisdiction in respect of any matter which the Privacy Commission is empowered by, or under, this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act

Jurisdiction.

45. On and from the appointed day, no court or authority shall have, or be entitled to exercise, any jurisdiction, powers or authority, except the Supreme Court and a High Court exercising powers under articles 32, 226 and 227 of the Constitution, in relation to matters over which the Privacy Commission has jurisdiction.

CHAPTER VII

Regulation by Data Controllers and Data Processors

Co-regulation by Data Controllers and the Privacy Commission.

46. (*1*) Without prejudice to the provisions of clause (d) of sub-section (2) of section 36, the Privacy Commission may, after a public consultation, formulate codes of conduct for the collection, storage, processing, disclosure or other handling of any personal data.

(*2*) No code of conduct formulated under sub-section (1) shall be binding on a data controller unless—

(*a*) it has received the written approval of the Chief Privacy Commissioner and at least two Privacy Commissioners; and

(*b*) it has received the approval, by signature of a director or authorised signatory, of the data controller.

Self-regulation by data controllers.

47. (*1*) The Privacy Commission may encourage data controllers and data processors to formulate professional codes of conduct to establish rules for the collection, storage, processing, disclosure or other handling of any personal data.

(*2*) No code of conduct formulated under sub-section (1) shall be effective unless it is registered, in such form and manner as may be prescribed, by the Privacy Commission.

(*3*) The Privacy Commission shall, for reasons to be recorded in writing, not register any code of conduct formulated under sub-section (*1*) that is not adequate to protect personal data.

Co-regulation and Self-regulation without prejudice to other remedies.

48. Any code of conduct formulated under this chapter shall be without prejudice to the jurisdiction, powers and functions of the Privacy Commission.

CHAPTER VIII

Offences and Penalties

Punishment for offences related to personal data.

49. (1) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any personal data shall be liable to fine which may extend to one crore rupees:

Provided that if the person commits the offence either intentionally, or with reckless disregard, he shall be liable for a term of imprisonment which may extend upto three years, and shall also be liable to fine.

(*2*) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes, discloses or otherwise handles any sensitive personal data shall be liable to fine which may extend upto ten crore rupees:

Provided that if the person committs the offence either intentionally, or with reckless disregard, he shall be liable for a term of imprisonment which may extend upto five years and shall also be liable to fine.

Punishment for offences related to interception of communication.

50. Whoever, except in conformity with the provisions of this Act, intercepts, or causes the interception of, any communication of another person shall be liable to a fine which may extend upto one crore rupees:

Provided that if the person commits the offence either intentionally, or with reckless disregard, he shall be liable for a term of imprisonment extending upto three years, and shall also be liable to fine.

Punishment for offences related to surveillance.

51. Whoever, except in conformity with the provisions of this Act, orders or carries out, or causes the ordering or carrying out, of any surveillance of another person shall be liable to a fine which may extend to ten crore rupees:

Provided that if the person commits the offence either intentionally, or with reckless disregard, shall be liable for a term of imprisonment extending upto five years, and shall also be liable to fine.

Abetment and repeat offenders.

52. Whoever abets any offence punishable under this Act shall, if the act abetted is committed in consequence of the abetment, be punishable with the punishment provided for that offence.

Offences by companies.

53. (*1*) Where an offence under this Act has been committed by a company, every person who, at the time of the offence was committed, was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

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

(*2*) Notwithstanding anything contained in sub-section (1), 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.

Cognizance.

54. Notwithstanding anything contained in the Code of Criminal Procedure, 1973, the offences under this chapter shall be treated as cognizable and non-bailable.

General penalty.

55. Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, including an order of the Chief Privacy Commissioner or otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to one crore rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend upto ten lakh rupees for every day after the first during which he has persisted in such failure or contravention.

Punishment to be without prejudice to any other action.

56. The award of punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under this Act with respect to such contravention.

CHAPTER IX

MISCELLANEOUS

Protection of action taken in good faith.

57. No suit or other legal proceeding shall lie against the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner, Privacy Commissioner or any person acting under the direction either of the Central Government, State Government, Privacy Commission, Chief Privacy Commissioner or Privacy Commissioner 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.

58. (*1*) 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.

(*2*) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Overriding effect.

59. Subject to the provisions of the Schedule to this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

Power to make rules.

60. (*1*) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(*2*) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for—

(*a*) the notification of theft, loss or damage under sub-section (*4*) of section 11;

(*b*) the notification of disclosure under sub-section (*4*) of section 13;

(*c*) the application by an intelligence organisation under sub-section (*2*) of section 15;

(*d*) the application to intercept a communication under sub-section (*1*) of section 18;

(*e*) the application to renew an interception of communication under sub-section (*2*) of section 20;

(*f*) the notification of an interception of communication under sub-section (*1*) of section 21;

(*g*) the application to not inform under sub-section (*2*) of section 21;

(*h*) the application to store information obtained as a result of any interception of communication under sub-section (*2*) of section 24;

(*i*) the application to carry out surveillance under sub-section (*3*) of section 26;

(*j*) notification to the general public under sub-section (*2*) of section 27;

(*k*) the application to renew surveillance under sub-section (*2*) of section 28;

(*l*) the notification of surveillance under sub-section (*1*) of section 29;

(*m*) the application to not inform under sub-section (*2*) of section 29;

(*n*) the application to store information obtained as a result of surveillance under sub-section (*2*) of section 32;

(*o*) salaries, allowances and other terms and conditions of service of the Chief Privacy Commissioner, Privacy Commissioners, Secretaries and other members, staff and employees of the Privacy Commission;

(*p*) procedure to be followed by the Privacy Commission;

(*q*) powers and duties of Secretaries, officers and other employees of the Privacy Commission;

(*r*) the effective implementation of this Act.

(*3*) 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 period of thirty days which may be comprised in one session or in two successive sessions and if before the expiry of the session in which it is so laid or the session immediately following, both Houses agree in making any modification in the rule, or both Houses agree that the rule shuold not be made, the rule shall thereafter have effect only in such mofidied 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.

THE SCHEDULE

1. Statutes, provisions whereof, shall have to comply with the requirements of this Act—

(*a*) Sections 43A, 69, 69B, 72 and 72A of the Information Technology Act, 2000.

(*b*) Sections 28, 29, 30, 31, 32 and 33 of the AADHAAR (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

(*c*) Section 5(*2*) of the Indian Telegraph Act, 1885.

(*d*) Section 21 of the Prevention of Money Laundering Act, 2002

(*e*) The Census Act, 1948.

2. Statutes, provisions whereof shall not be required to comply with the provisions of this Act—

(*a*) The Representation of the People Act, 1951.

(*b*) The Right to Information Act, 2005.

STATEMENT OF OBJECTS AND REASONS

Our country is at the threshold of a new technological revolution, marrying welfare with programmes of digitization for the quick and effective delivery of government services and benefits from various schemes. For this process, ranging from electronic banking to the transfer of subsidies, vast amounts of data are collected from our citizens, the integrity of which must be protected. This data can be used for seemingly innocuous purposes such as targeted advertising but also for provision of essential services such as ration, credit, insurance, and more, while unprotected and in the wrong hands, it could also cause damage to the interests of the individual.

Beyond its commercial exploitation there is also an inherent equation of power when a person or entity possesses data and information concerning another individual or groups of individuals. Today, most such interactions are unregulated and put the users of internet and technological services at risk, and this risk will only grow with more and more digitization and as technological involvement in the delivery of services to citizens develops.

Many concerns arise from the absence of a comprehensive data protection and privacy statute which provides rights to individuals in a data governed world. This has been recognized by past efforts of the Government of India notably by the Report of the Group of Experts on Privacy chaired by Justice A.P. Shah, Former Chief Justice, Delhi High Court. Drawing on the recommendations of this expert group, global best practices and also the unique factors that exist locally, this Data Privacy And Protection Bill aims to provide a comprehensive law to protect privacy and data collected from our citizens.

This bill puts a person in control of his/her own data and further permits them to make an informed choice concerning its use. The Bill further provides an industry friendly model of co-regulation that aims to foster a higher degree of certainty for the private sector. The concerns of government are also sought to be addressed with a balanced provision for interception and access, making special provisions to safeguard the security of the State. The aims and objectives of the bill are sought to be implemented by an autonomous privacy commission.

The Data Privacy and Protection Bill, 2017 aims to protect and promote our constitutional ideals in a networked, increasingly digitized society.

Hence this Bill.

NEW DELHI;
July 2, 2017

SHASHI THAROOR

FINANCIAL MEMORANDUM

Clause 33 of this Bill provides for establishment of the Privacy Commission. It also provides for appointment of a Select Committee to fill vacancies in the Privacy Commission. Clause 34 provides for salaries and allowances payable to the Chief Privacy Commissioner and allowances or remuneration payable to the Privacy Commissioners. Clause 36 provides for constitution of an adhoc Committee to serve the functions of the Privacy Commission. Clause 37 provides for the appointment of a secretary, officers and other employees of the Privacy Commission. The Bill, therefore, if enacted, would involve expenditure from the Consolidated Fund of India. It is estimated that a recurring expenditure of about rupees six hundred crore per annum from the Consolidated Fund of India.

A non-recurring expenditure of about rupees one hundred and twenty five crore is also likely to be involved.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 60 of the Bill empowers the Central Government to make rules for carrying out the purposes of this Bill. 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 establish an effective regime to protect the right to privacy of data all natural person; to set out conditions of surveillance and interception of communications of natural persons; and to constitute a Privacy Commission and for matters connected therewith or incidental thereto.

———

(*Dr. Shashi Tharoor, M.P.*)

GMGIPMRND—1121LS(S3)—28.07.2017.