SAVE OUR PRIVACY

INDIAN PRIVACY CODE, 2018

A

BILL

To establish an effective regime to protect the fundamental right to privacy of all natural persons and personal data concerning them, to set out conditions upon which surveillance of natural persons and interception of communications may be carried out, to constitute a Privacy Commission, and for matters connected therewith and incidental thereto.

WHEREAS the right to privacy is an inalienable fundamental right of all natural persons indispensable to the preservation of human dignity, personal autonomy and the exercise of constitutional liberties;

AND WHEREAS the need to protect privacy has only 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 legislation;

SAVE OUR PRIVACY

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

BE IT ENACTED by Parliament in the Sixty-Eighth Year of the Republic of India as follows –

CHAPTER I

PRELIMINARY

1. Short title, extent and commencement

(1) This Act may be called the Indian Privacy Code, 2018.

(2) It extends to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person, wherever located.

(3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint.

2. Definitions. –

(1) In this Act and in any rules made thereunder, unless the context otherwise requires, –

(a) "aggregate", with its grammatical variations and cognate expressions, in relation to personal data, means adding, removing, filtering, mixing, combining or recombining records of data.

SAVE OUR PRIVACY

(b) “anonymise” means, in relation to personal data, the irreversible removal or alteration 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;

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

-by the Central Government or a Union Territory Administration, the Central Government;

-by a State Government, that State Government;

(d) “authorised officer” means an officer of a competent organization, 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 the communications of another person or carry out any surveillance of another person under this Act;

(e) “biometric data” means any data relating to the physical, physiological or behavioural characteristics of a natural person which allows the verification or authentication of that person’s identity including, but not restricted to, facial images, fingerprints, hand prints, foot prints, iris recognition, handwriting, typing dynamics, gait analysis and speech recognition;

(f) “Chief Privacy Commissioner” and “Privacy Commissioner” mean the Chief Privacy Commissioner and Privacy Commissioners appointed under section 47;

(g) “collect”, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person obtaining, or coming into the knowledge or possession of, any personal data of another person, whether directly or indirectly;

SAVE OUR PRIVACY

(h) “communication” means a word, 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 metadata in relation whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

(i) “competent organisation” means an organisation authorised by law to carry out surveillance and/or interception, and includes a public authority as listed in the Schedule to this Act;

(j) “consent” means unambiguous indication of a data subject’s agreement;

(k) “data” means as defined under Section 2(o) of the Information Technology Act, 2000;

(l) “data controller” means any person including appropriate government who, either alone, or jointly, or in concert with other persons, determines the purposes for which and the manner in which any personal data is processed;

(m) “data processor” means any person including appropriate government who processes any personal data on behalf of a data controller;

(n) “data subject” means a natural person who is a citizen under the Citizenship Act, 1955 or who has resided in India for a period or periods amounting in all to 182 days or more in the twelve months preceding the previous year.

(o) “deoxyribonucleic acid data” means all information, of whatever type, concerning the characteristics of a natural person that are inherited or acquired during early prenatal development;

(p) “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 which becomes irretrievable in whole or in part including information about the existence of such data itself;

SAVE OUR PRIVACY

(q) “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;

(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 (2 of 1974);

(t) “person” means and includes a natural person, a company, a firm, an association of persons, a public authority or a body of individuals, wherever located, 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) “prescribed” means prescribed by rules and regulations made under this Act, including as provided in Section 81;

(w) “Privacy Commission” means the body constituted under sub-section (1) of section 46;

(x) “Privacy Officer” means the Privacy Officer designated under sub-section (3) of section 34 and sub-sections (3) and (4) of section 42.

(y) “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, collection, aggregation, organisation, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction;

(z) “public authority” shall have the meaning ascribed to it under clause (h) of section 2 of the Right to Information Act, 2005 (22 of 2005);

(aa) “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;

(bb) “sensitive personal data” means data or metadata as to a person's -

(i) biometric data;

(ii) deoxyribonucleic acid data;

(iii) sexual preferences and practices;

(iv) medical history and health information;

(v) political affiliation;

(vi) membership of a political, cultural, social organisations including but not limited to a trade union as defined under Section 2(h) of the Trade Union Act, 1926;

(vii) ethnicity, religion, race or caste; and

(viii) financial and credit information, including financial history and transactions.

(cc) “State Privacy Commission” means the body constituted under sub-section (1) of Section 64;

SAVE OUR PRIVACY

(dd) “Surveillance and Interception Review Tribunal” means the bodies constituted under sub-section (1) of Section 69;

(ee) “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;

(ff) “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 about a person and their private affairs, including:

(i) directed surveillance that is covert surveillance undertaken for a specific investigation or operation even if the person surveilled was not specifically identified in relation to the surveillance operation;

(ii) inclusive surveillance which is covert surveillance carried out by an individual or surveillance device in relation to anything taking place in any private premises or private vehicle;

(iii) covert human intelligence gathering which is information obtained by a person who establishes or maintains a personal or other relationship with a person for a covert purpose of using it to obtain access to any personal information about that individual;

(iv) surveillance undertaken through installation and use of CCTV and other system which capture audiovisual information to identify or monitor individuals; but does not include collection of personal data under Sections 7, 10 and 11 of this Act;

(2) All other expressions used herein, as the case may be, shall have the meanings ascribed to them under the General Clauses Act, 1897 (10 of 1897) or the Code of Criminal Procedure, 1973 (2 of 1974).

SAVE OUR PRIVACY

CHAPTER II

RIGHT TO PRIVACY

3. Principles applicable to protecting privacy

(1) In exercising the powers conferred by this Act, regard shall be had to the following considerations, namely –

(i) that the right to privacy is a fundamental right essential to the maintenance of a democratic society and is recognised as a fundamental human right provided under Part III of the Constitution and various international treaties to which India is a party;

(ii) that personal data with its attributes belongs solely to the natural person to whom it pertains who are referred to as the data subjects for the purposes of this act;

(iii) that personal data of data subjects shall be processed fairly and lawfully and in no circumstance shall be processed unless the conditions under this act are met;

(iv) that intrusions into privacy should always be for lawful purposes measured by principles of legality, necessity and proportionality;

(v) that unless as otherwise expressly provided the consent of data subjects for a specific purpose will be a mandatory condition prior to storage and processing of her personal data;

SAVE OUR PRIVACY

(vi) that personal data is required by data controllers, and data processors, to enable good governance and the delivery of goods and provision of services without undue delay which may be provided by a meaningful, revocable and accountable notice and consent framework;

(vii) that the right to privacy shall not be used to limit or fetter the fundamental right to freedom of speech and expression journalists and the press or accountability of the government and public institutions under the right to information laws;

(viii) that privacy must be upheld by a statutory body that is independent, impartial, well resourced and free from unwarranted influence.

4. Rights to privacy

(1) Without prejudice to the generality of the provisions contained herein, all natural persons shall have a right to privacy which shall be implemented as per principles laid down in Section 3 of this Act.

(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.

5. Exemption

(1) Nothing in this Act shall apply to –

(i) the collection, storage, processing or dissemination by a natural person of their own personal data; or

SAVE OUR PRIVACY

(ii) the collection, storage, processing or dissemination by a natural person of personal data for a strictly non-commercial purposes which may be classified as open data by the Privacy Commission;

(iii) Surveillance by a resident of their own residential property, or

(iv) Subject to obtaining the Privacy Commission's exemption under sub-section (3) of section 15, the collection, storage or processing of anonymized data for non-commercial purposes or by any entity for academic, journalistic, research, statistical or archival purposes as required under the provisions of an Act of Parliament.

Explanation. - For the purposes of this section, "non-commercial purposes" means permissible acts and omissions which as may be prescribed by the Privacy Commission through processes of public consultation with due regard to academics, civil society, experts and professional bodies.

CHAPTER III

PROTECTION OF PERSONAL DATA

PART A

NOTICE BY DATA CONTROLLERS

6. Transparency in form and substance in all communications by Data Controllers

SAVE OUR PRIVACY

(1) All communications by Data Controllers shall be complied with in the following manner:

(i) In a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a person below 13 years of age.

(ii) Information shall be provided in writing, or by other means, including, where appropriate, by electronic means and when requested by the data subject, may be provided orally when deemed appropriate as per regulations that may be made by the Privacy Commission.

(iii) Requests for information by Data Subjects to Data Controllers shall be complied with promptly, ideally within a period of two working days noting acknowledgment of receipt and communicating the timelines for compliance that shall have a limit of one month (30 days) from the date of receipt of the request for information.

Provided that all communications by the Data Controllers including but not limited to the rights of Data Subjects under this part shall may be refused when the Data Controller is, unable to identify or has a well founded basis for reasonable doubts as to the identity of the Data Subject or are manifestly unfounded, excessive and repetitive, with respect to the information sought by the Data Subject. In all such instances the Data Controller will provide reasons for failure to comply with the request which shall be subject to remedies including appeal as provided under provisions of this Act.

(i) Information shall include specific reference to the rights and remedies, include availability of measures for rectification, restriction and erasure as provided to Data Subjects under this Act

SAVE OUR PRIVACY

(2) Special measures, which meet the satisfaction of the Privacy Commission, shall be taken in order to ensure that such information provided by Data Controllers is accessible to all data subjects, including those who -

i. are illiterate; and
ii. suffer impaired or total lack of vision or hearing; and
iii. fall into any other category requiring special measures, as may be prescribed by the Privacy Commission.

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

(3) The Privacy Commission may frame regulations to ensure compliance by Data Controllers of the rights to transparency and modalities of Data Subjects.

PART B

CONSENT OF DATA SUBJECTS

7. Prior consent necessary to the collection of data

(1) Data shall be collected by a Data Controller from a Data Subject only after effecting consent.

(2) Consent shall be deemed to have been validly effected only if it is:

(i) Obtained from a person competent to contract in terms of section 11 of the Indian Contract Act, 1872;

SAVE OUR PRIVACY

(ii) Free, in the terms of section 14 of the Indian Contract Act, 1872;

(iii) Informed, that is made with full knowledge of risks involved and the alternatives available;

(iv) Obtained prior to all data collection, except in the cases expressly excluded by section 11;

(v) Voluntarily given through an express and affirmative act and is recorded in writing;

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

(i) if the written declaration of consent was given in a manner where it also concerned other matters, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language;

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

(iii) the means for its withdrawal can be employed with the same ease as the means by which it was obtained.

(3) Specific and limited as to purpose and duration, and;

(4) Collected in a manner as prescribed by the Privacy Commission

Explanation 1: Consent will 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 will be be deemed to be specifc 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 such expanded purposes

(iii) in a manner as prescribed by the Privacy Commission

8. Special provisions in respect of data subjects lacking legal capacity to give consent

(1) Consent in relation to personal data, excluding sensitive personal data which is strictly necessary for the provision of emergency medical services, relating to minors shall be effective only if -

(2) In respect of minors above the age of 13, where it is obtained from a parent, legal guardian, or such other person acting in loco parentis as the case may be, after the minor is informed by the Data Controller in a simple and explanatory manner of the need for care in handling data concerning herself.

Provided that upon attaining majority, the Data Subject is entitled to:

(i) be duly informed of the terms upon which personal data relating to her has been collected;

(ii) alter or rescind the terms on consent; and

(iii) require the destruction of all personal data relating to her.

(3) Consent in relation to personal data relating to Data Subjects of unsound mind shall be effective only if it is obtained from a legal guardian, or such other person expressly empowered to act on behalf of her under any law for the time being in force.

Provided that where the unsoundness of mind is temporary, the Data Subject is entitled to withdraw consent given in her behalf during the period of such unsoundness.

(4) Consent in relation to personal data relating to Data Subjects of any other class of natural persons identified by the Privacy Commission shall be effective only if it satisfies all conditions set out in rules prescribed in that regard by the Privacy Commission.

(5) All rights and entitlements accorded to data subjects under this Act will be deemed to accrue to Data Subject as may be entitled to consent on behalf of her.

Explanation: Where no person acting on behalf of a data subject falling into any of the classes covered by this section can be identified despite the best efforts of the data controller or data processor, the State Privacy Commission, being accountable in a fiduciary capacity to the data subject, shall act on behalf of her.

9. Special provisions in respect of data subjects unable to give consent

SAVE OUR PRIVACY

(1) Consent in relation to personal data relating to Data Subjects who are competent but temporarily unable by reason of their circumstances to give consent shall be effective only if it is obtained in relation to purposes which are strictly necessary to uphold or advance the interests of the Data Subject or to the interests of the public, and the following conditions are met –

(i) In respect of Data Subjects who are declared missing under law and for period they are missing, it is obtained from their nearest living relative, and where all reasonable means to contact their nearest living relative have been demonstrably exhausted, it is obtained from any person legally empowered to act in their behalf, or as a last resort, the appropriate State Privacy Commission in whose jurisdiction she was last resident;

(ii) In respect of data subjects who are detained, where all reasonable means to contact them, their nearest living relative have been demonstrably exhausted, it is obtained from any person legally empowered to act in their behalf, or as a last resort, the Appropriate State Privacy Commission in whose jurisdiction she was last resident;

(iii) In respect of Data Subjects who are temporarily incapable for medical reason and for the duration of their temporary incapacity, it is obtained from their nearest living relative, and where all reasonable means to contact their nearest living relative have been demonstrably exhausted, it is obtained from any person legally empowered to act in their behalf, or as a last resort, the appropriate State Privacy Commission in whose jurisdiction she was last resident

Provided that when the inability to consent passes and where the personal data collected during the period of inability has not been anonymised, the data subject is entitled to -

SAVE OUR PRIVACY

(i) alter or rescind the consent given on her behalf in all cases, and
(ii) request the destruction of all records of personal data relating to her.

(2) Consent in relation to personal data relating to Data Subjects who are unable, for reasons of death, and have not named a nominee to give, shall be effective only if it is obtained from-

(i) the nearest living relative; or

(ii) where all reasonable measures to identify nearest living relative fail, the State Privacy Commission of the state in which the person was last resident.

10. Collection of personal data

(1) No person, including a data controller and data processor, shall collect any personal data without obtaining the 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 prescribed by the Privacy Commission, inform the data subject free of any direct or indirect charges, to whom it pertains of the following details in respect of their personal data, namely–

(i) when it will be collected;

(ii) its content and nature;

(iii) the purpose of its collection;

(iv) the purpose and manner in which it will be used;

(v) the persons to whom it will be made available;

(vi) the duration for which it will be stored;

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

(viii) the security practices and other safeguards, if any, to which it will be subject;

(ix) the privacy policies and other policies, if any, that will protect it;

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

(xi) the time and manner in which it will be destroyed, or the criteria used to 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: determine that time period;

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

(xiii) the identity and contact details of the data controller and data processor

(4) 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, except where it is an essential service as

SAVE OUR PRIVACY

provided under Section 13, or the fulfillment of a lawful contract, not deliver that good or deny that service or fulfill that contract to the data subject who withdrew the grant of consent easily and at any point during the duration of a service.

11. Collection of personal data without prior consent

(1) Personal data may be collected or received from a third party by a Data Controller the prior consent of the data subject only if it is –

(i) necessary for the provision of an emergency medical service or essential services as provided under Section 13 to the Data Subject;

(ii) strictly necessary to prevent, investigate or prosecute a cognizable offence.

(iii) exempted by the Privacy commission as per provisions relating to interception and surveillance.

Provided that for sub-sections (a) and (b) the data subject shall be duly informed in simple language and through a medium perfectly accessible to her, in a manner as prescribed by the Privacy Commission, at the earliest possible opportunity of the extent of personal data collected, and the processing and uses that it was put to in the course of meeting the purpose of the collection.

(2) All personal data collected without prior consent shall be destroyed as soon as the purpose for which it is collected expires.

Provided that where effective consent is obtained in terms and as per the safeguards under the Act at the earliest possible opportunity and no later than 7 days from the date of the collection of the personal data, such personal data may continue to be stored and processed.

SAVE OUR PRIVACY

12. Special provisions in respect of data collected prior to the commencement of this Act

(1) All data collected, processed and stored by data controllers and data processors prior to the date on which this Act comes into force shall be destroyed within a period of two years from the date on which this Act comes into force.

(2) Nothing in sub-section (1) shall apply where:

(i) Consent in terms which satisfies all the requirements for effective consent under this Act is obtained afresh within the aforementioned period of two years; or

(ii) The personal data collected prior to the commencement of this Act was anonymised in such a manner as to make reer-identification of the data subject absolutely impossible.

Explanation- For the purpose of this section only, consent shall be deemed to have been obtained if the data subject does not explicitly withdraw consent, on the basis of a specific notification in this regard, provided by data controller to the data subject, in a manner as prescribed by the Privacy Commission, within the aforementioned period of two years.

PART C

FURTHER LIMITATIONS ON DATA CONTROLLERS

13. Bar on denial of essential services

(1) No essential services, by whosoever provided, including -

SAVE OUR PRIVACY

(i) entitlements under the Public Distribution System including but not limited to the provisions under the National Food Security Act, 2013;

(ii) the provision of medical care to minors, expectant mothers or those requiring emergent or life-saving care;

(iii) social security benefits, including pension, gratuity and provident fund;

(iv) benefits under the Mahatma Gandhi National Rural Employment Guarantee Act, 2005;

(v) services provided to effectuate provisions of Part III or Part IV of the Constitution;

(vi) any other service prescribed by the Central Government;

shall be withheld on the ground that consent to share personal data in a particular manner for the purpose of identification, has not been obtained or has been withheld or such data has not been collected at the time the data subject claims the service;

Provided that the data subject shall be entitled to damages where an essential service has been denied.

Provided further that the data controller or processor shall accept any alternate means for identification, wherever available per the choice of the data subject, and the data subject shall be entitled to exemplary damages where an essential service has been denied despite the existence of pre-existing alternative means of identifying the data subject.

(2) Where an essential service is provided under sub-section (1) and the provider of the said service can demonstrate grave and irreparable injury arising directly from the unavailability

of personal data in respect of which consent was sought, it may approach the Privacy Commission for relief or seeking exemption.

14. Storage and destruction of personal data

(1) No person 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.

Provided that where the purpose of collection is the provision of essential services under Section 13 or of banking as provided under Section 5(b) of the Banking Regulation Act, 1949, the data subject shall be duly informed in terms to be prescribed by the Privacy Commission of the impending destruction of the data

(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 –

(i) 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;

(ii) it is adduced for an evidentiary purpose in a legal proceeding; or

SAVE OUR PRIVACY

(iii) it is required to be stored for historical, statistical or research purposes under the provisions of an Act of Parliament and specified in a manner as prescribed by the Privacy Commission:

Provided that only such amount of personal data that is necessary to achieve the purpose of storage under this subsection 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 subsection shall, to the extent possible, be anonymised.

15. Processing of personal data

(1) Save as provided in sub-section (2), 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) 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 only if –

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

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

(iii) it is necessary to prevent an imminent threat to the security of the State or public order and the fact of such threat is recorded in writing by a competent organization which anticipates such a threat; or

(iv) it is necessary to prevent, investigate or prosecute a cognizable offence.

SAVE OUR PRIVACY

(2) Notwithstanding anything contained in this section personal data may be anonymized, as a measure to enhance the security of the data and the privacy of the data subject.

Provided that anonymized data may be processed or disseminated only if the data controller has demonstrated to the Privacy Commission that it is impossible to identify the data subject to whom it relates and sought a specific exemption.

Provided further that where the Privacy Commission is satisfied that the personal data has been satisfactorily anonymized, the Privacy Commission may grant an extension on the permissible period of storage and disclosures for specified purposes in addition to those in respect of which effective consent was obtained.

16. Security of personal data and duty of confidentiality

(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) 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 generality of the provisions of this section and notwithstanding any law for the time being in force, 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 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.

(5) Any person, who collects, receives, stores, processes, or otherwise handles any personal data shall report all violations of provisions of this Chapter to the Privacy Commission, that are brought to its notice, or are reasonably expected to be known to such persons.

17. Transfer of personal data outside the territory of India

(1) Subject to the provisions of this section, personal data that has been collected according to this Act may be transferred by a data controller to a data processor located in India, if the transfer is pursuant to an agreement that demonstrably and expressly binds the data processor to same or stronger conditions and 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 controller shall transfer personal data outside the territory of India or to an international organisation unless any one of the following conditions is met:

(i) The Central Government has issued a notification indicating it has decided that the country, territory, or international organization in question has demonstrated that it ensures an adequate level of protection of privacy and personal data in a manner which is in no way incompatible with the privacy principles contained in Section 3 of this Act,

Provided that any such notification of an adequacy decision shall only be issued by the Central Government after due consultation with the Privacy Commission and its Office of Data Protection, and after having taken inputs from such stakeholders and experts as the latter may recommend; or

(i) The transfer by the data controller to a data processor located outside India is pursuant to an agreement that demonstrably and binds the recipient of the personal

SAVE OUR PRIVACY

data to the same or stronger conditions and measures in respect of the storage, processing, destruction, disclosure, and other handling of the personal data as contained in this Act; or

(ii) The data controller has assessed all the circumstances surrounding the transfer of personal data in question to the third country, territory, or international organization and concluded that appropriate legal instruments and safeguards exist to protect the data, and informed the Office of Data Protection of the Privacy Commission of such transfers of data

Provided that in informing the Privacy Commission, the data controller must ensure that it can provide documentation on request that includes the particulars regarding

(i) the date and time of the transfer,

(ii) the name of and any other pertinent information about the data processor,

(iii) the justification for the transfer, and

(iv) a description of the personal data transferred

(v) the existing legal instruments and safeguards for data protection by which the data processor is bound.

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

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

SAVE OUR PRIVACY

(5) Any data controller who transfers personal data outside the territory of India shall continue to be liable for the compliance with the provisions of this Act notwithstanding the fact that the personal data in question is being processed outside the country.

Explanation: Such duties shall include, but not be limited to:

a) ensuring that any recipient of such transferred personal data takes appropriate steps to ensure compliance with the provisions of this Act

b) reporting any breach to the Privacy Commission notwithstanding the transfer of such data outside the territory of India

18. Disclosure of personal data

(1) Save as provided in this Chapter, no person including the Data Controller 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 including the Data Controller shall disclose any personal data without obtaining the prior effective consent of the data subject, 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 including the Data Controller 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: –

(i) when and to whom it will be disclosed;

(ii) the purpose of its disclosure;

(iii) the security practices and other safeguards, if any, to which it will be subject;

SAVE OUR PRIVACY

(iv) the privacy policies and other policies, if any, that will protect it;

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

(vi) any other details prescribed by rules which may be prescribed by the Privacy Commission.

(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.

(5) Any disclosure of personal data made contrary to the provisions of this Act shall be notified to the Data Subject and Privacy Commission.

19. Special provisions for sensitive personal data

(1) Notwithstanding anything contained in this Act and the provisions of any other law for the time being in force –

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

(ii) no person shall store sensitive personal data for a period longer than is strictly necessary to 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;

(iii) no person shall process sensitive personal data for any purpose other than the purpose for which it was collected or received;

(iv) 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.

(2) In addition to the requirements set out under sub-clause (1), the Privacy Commission shall set out additional protections in respect of:

(i) sensitive personal data relating to data subjects who are minors;

(ii) biometric and deoxyribonucleic acid data; and

(iii) financial and credit data.

20. Special provisions for data impact assessment

(1) Where the data controller uses, directly or indirectly any new technology, it shall be obligated to assess the risks to the data protection rights under this act which result from such processing.

(2) The data controller shall conduct an internal process of a data protection impact assessment which shall include a systematic and extensive evaluation of the personal aspects relating to data subjects especially the impact on their legal rights which result from the new technology.

(3) All data impact assessment reports will be submitted periodically to the State Privacy commission as per the rules and regulations made under this act.

SAVE OUR PRIVACY

Explanation: "new technology" shall include any pre-existing technology used for anew purpose through an iterative process by which any existing or pre-existing process or output is substantially changed.

PART C

RIGHTS OF A DATA SUBJECT

21. Right to access for data subject

(1) The data subject shall have the right to obtain from the Data Controller confirmation as to whether any personal data concerning her is collected or processed, and, where any such personal data has been collected or processed by the Data Controller, access to the personal data shall be granted alongwith the following information:

(i) the purposes of the storage and processing;

(ii) the categories of the personal data concerned;

(iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular to determine that period;

(iv) 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;

(v) the right to lodge a complaint with a supervisory authority;

(vi) where the personal data are not collected from the data subject, any available information as to their source;

(vii) the existence of automated decision making, including profiling.

(2) When the personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the safeguards as per provisions of this Act.

(3) The Data Controller shall provide a single copy of the personal data undergoing processing to the Data Subject and additional copies may be subject to additional charges on a concessional and reasonable basis.

(4) The right to access data by a Data Subject shall be in addition to the notifications and existing obligations of Data Controllers.

22. Right to rectification for Data Subjects and obligations of Data Controllers

(1) The Data Subject shall have the right to obtain from the Data Controller promptly the rectification of inaccurate personal data concerning her.

(2) Any Data Controller 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.

(3) No Data Controller 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.

SAVE OUR PRIVACY

(4) Specific notification shall be provided by the Data Controller to the Data Subject of any rectification of personal data pertaining to the Data Subject unless this proves impossible or involves disproportionate effort.

23. Right to erasure and destruction of personal data

(1) The Data Subject shall have a right to request erasure and destruction of data at any time, and Data Controllers and processors shall comply with such requests, within a timeframe, manner and mode to be prescribed by the Privacy Commission.

(2) The Data Subject shall have the right to obtain from the Data Controller the erasure of personal data concerning her without any delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds apply:

(i) The personal data is no longer necessary in relation to the purposes for which it was collected or processed;

(ii) The Data Subject withdraws consent as per the provisions of this act and no other legal ground for processing continues to exist;

(iii) The personal data has been unlawfully processed.

(2) The provisions of this section shall not apply when the storage or processing is determined by the Privacy Commission to be:

(i) for exercising the to right of speech and freedom of expression which includes the right to receive information, especially about public personalities, officials or matters of public interest.

(ii) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and the erasure is likely to be or render impossible or seriously impair such objectives.

(iii) for the establishment, exercise or defense of any legal proceedings.

(iv) as per the provisions of this act including but not limited to anonymised data as contained under Section 15.

(3) Specific notification shall be provided by the Data Controller to the Data Subject of any erasure or destruction of personal data pertaining to the Data Subject unless this proves impossible or involves disproportionate effort.

24. Right to restriction of processing

(1) The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies-

(i) the accuracy of the personal data is contested by the data subject, for a period enabling the Data Controller to verify the accuracy of the personal data;

(ii) the processing is unlawful and the data subject opposes the erasure of the Personal Data and requests the restriction of its use instead;

(iii) the Data Controller no longer needs the personal data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defense in legal proceedings;

(iv) the Data Subject has objected to processing pending verification whether the legitimate grounds of the Data Controller override those of the Data Subject.

(2) When the processing has been restricted under this provision, such personal data shall, with the exception of storage, only be processed with the Data Subject's consent or for the establishment, exercise or defense in legal proceedings or for the protection of the rights of another natural person.

(3) A Data Subject who has obtained restriction of processing pursuant to this section shall be informed by the Data Controller before the restriction of processing is lifted.

25. Right to object

(1) The Data Subject shall have the right to object, on grounds relating to her particular situation, at any time to processing of personal data concerning her which is based on the principles for protection of privacy as provided under Section 3 of the Act.

(2) The Data Controller shall in addition to its other obligations, for communication of notices to the Data Subject under this act shall at the latest at the time of the first communication with the Data Subject provide notice to the Data Subject of its right to object, clearly and separately from other information.

26. Right to portability of personal data

(1) The data subject shall have the right to receive all personal data concerning her from any data controller within a reasonable time and in a structured, commonly used and machine-readable format upon request.

(2) Except where it is expressly precluded by any law for the time being in force, the data subject shall have the additional right to receive the output of all processing of personal data concerning her within a reasonable time.

(3) The data controller shall not hinder in any manner the transfer by the data subject, of the personal data, to any other person.

SAVE OUR PRIVACY

(4) The data subject shall have the right to request that the personal data be transmitted directly from one controller to another, in all instances where it is technically feasible, and the data subject be informed upon the completion of the said transmission.

Provided that no transmission will be deemed to be complete until all records of the data so transmitted as per the instructions of the data subject are then destroyed by the data controller to whom request is made.

(5) Where the data controller claims that it is not technically feasible to transfer data in the manner provided for under sub-section (4) and the data subject challenges such a claim in terms of rules prescribed by the Privacy Commission in this regard, the burden to demonstrate a lack of technical feasibility to transfer falls upon the data controller.

27. Right to seek exemption from automated decision-making

(1) The data subject in addition to her rights with respect to processing of personal data will specifically have the right to seek exemption from decisions based solely on automated processing including profiling, which produces legal effects concerning or significantly affecting her.

(2) The provisions of sub-section (1) will apply, only if the automated decision:

(i) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(ii) is based on the data subject's express and explicit consent;

(iii) is provided a case by case exemption in cases by the Privacy Commission having regard to the principles as provided under Section 3 of this Act;

SAVE OUR PRIVACY

Explanation: "case by case exemption" shall only apply to instances of an individual person and shall not include any exemption for a category or a class of Personal Data.

(3) In the instance of the inapplicability of sub-section (1) as provided for in sub-section (2) or in any other instance as provided by law, the data controller will have an obligation to provide additional safeguards with specific provisions for the right of the Data Subject to obtain human intervention of a natural person on the part of the Data Controller for providing an effective process of hearing and contesting decisions.

(4) All decisions made by automated decision-making made by data controllers shall be open to legal remedies including appeals as provided under this Act.

CHAPTER IV

INTERCEPTION AND SURVEILLANCE

28. Special provisions for competent organizations

(1) All provisions of Chapter III shall apply to personal data collected, processed, stored, transferred or disclosed by competent organizations unless when done as per the provisions under this chapter;

(2) A competent organization seeking to exclude the application of provisions of Chapter III with respect to personal data collected, processed, stored, transferred or disclosed by itself, shall prefer an application with the Privacy Commission, in a manner prescribed by the Privacy Commission.

(3) An application under sub-section (2) shall specify:

SAVE OUR PRIVACY

(i) the specific personal data sought to be exempted from provisions of Chapter III of this Act;

(ii) the reasons as to why the same is necessary to prevent a reasonable threat to security of state or public order or to prevent, investigate or prosecute a cognizable offence; and

(iii) the specific time period during which the exemption is sought.

(4) No competent organisation shall process or store any personal data without implementing measures to ensure 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.

(5) Notwithstanding any provisions of the Indian Evidence Act, 1872 any personal data collected, processed, stored, transferred or disclosed by a competent organization in contravention of this Act will be inadmissible in legal proceedings before any court of law.

29. Bar against interception of communications

(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 appropriate Surveillance and Interception Review Tribunal.

(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.

30. Prior authorisation by the appropriate Surveillance and Interception Review Tribunal

SAVE OUR PRIVACY

(1) An authorised officer of a competent organisation seeking to intercept any communication of another person shall prefer an application, in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, to the appropriate Surveillance and Interception Review Tribunal.

(2) The appropriate Surveillance and Interception Review Tribunal may, if it 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.

(3) Prior to issuing an order for interception of any communication, the appropriate Surveillance and Interception Review Tribunal, shall satisfy itself that all other lawful means to acquire the information sought to be intercepted have been exhausted and that the proposed interception is necessary and proportionate, reasonable 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 Office for Surveillance Reform of the Privacy Commission.

(5) Any interception involving the infringement of the privacy of individuals who are not the subject of the intended interception, or where communications relate to medical, journalistic, parliamentary or legally privileged material may be involved, shall satisfy additional conditions including the provision of specific prior justification in writing to the Office for Surveillance Reform of the Privacy Commission as to the necessity for the interception and the safeguards providing for minimizing the material intercepted to the greatest extent possible and the destruction of all such material that is not strictly necessary to the purpose of the interception.

31. Authorisation by Home Secretary in emergent circumstances

SAVE OUR PRIVACY

(1) Notwithstanding anything contained in Section 30, if the Home Secretary of the appropriate government is satisfied that an imminent grave threat to the security of the state or public order exists, she 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 appropriate Surveillance and Interception Review Tribunal 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.

(4) Upon receipt of notification under subsection (3), the Surveillance and Interception Review Tribunal, may, recall the order on grounds of lack of an imminent and grave threat to the security of state or public order, or on absence of ground mentioned in sub-section (2) of section 30, and may also order for damages in instances of abuse to be paid to the natural person whose communication was intercepted under the order so recalled.

32. Duration of interception

(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 the order.

SAVE OUR PRIVACY

(2) The appropriate Surveillance and Interception Review Tribunal, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, renew, for a period not exceeding sixty days, any order for interception of any communication if it is satisfied that the conditions upon which the original order was issued continue to exist.

Provided that where interception of communication, under orders passed under this Chapter, including orders for renewal, has been carried out for a cumulative period of 6 months, whether in succession or not, any application for further renewal, shall be accepted, if in addition to the ground mentioned in this subsection, the competent organization is able to demonstrate the need for such continued interception.

33. Duty to inform the person concerned

(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 or any interception of communication carried out before the Act came into operation, the authorised officer who carried out the interception of communication shall, in writing in such form and manner as may be prescribed by Central Government in consultation with the Privacy Commission, notify, with reference to the relevant order of the Surveillance and Interception Review Tribunal, each person whose communication was intercepted of the fact of such interception and duration thereof.

(2) The Surveillance and Interception Review Tribunal 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) would 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:

SAVE OUR PRIVACY

Provided that 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 cessation of which the duty to inform under sub-section (1) will operate.

34. Security and duty of data security and privacy

(1) 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 have a duty of data security and privacy with respect to it.

(2) 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 data security and privacy of all information obtained as a result of an interception of communication, including from theft, negligence, loss or unauthorised disclosure.

(3) Every competent organisation 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 ensuring that all interceptions of communications carried out by that competent organisation are in compliance with the provisions of this Chapter.

35. Disclosure of intercepted communications

(1) In addition to the existing obligations and duties for lawful interception, no person shall disclose to any person, other than the person whose communication has been intercepted, 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.

SAVE OUR PRIVACY

(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 organisation.

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.

36. Storage and destruction of intercepted communications

(1) Subject to sub-section (2), no person shall store any data, 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 and upon expiry of such period, shall destroy the data so stored.

(2) The Surveillance and Interception Review Tribunal may, on an application made in such form and manner as may be prescribed by the Privacy Commission, if it is satisfied that it is necessary to:

(i) prevent a reasonable threat to the security of the state; or

(ii) public order; or

(iii) prevent, investigate or prosecute a cognisable offence in an ongoing legal proceeding and is authorized by a court order to that effect;

SAVE OUR PRIVACY

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 and shall not be destroyed.

(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 14 with respect to such data.

37. Bar against surveillance

(1) 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 of 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 identification of welfare beneficiaries, the security of state, interests of public order or to prevent, investigate or prosecute a commission of a cognisable offence.

(2) The appropriate Surveillance and Interception Review Tribunal shall have the power to issue appropriate directions, including for cessation of any activity, being carried out by a person, including a statutory authority, which is in contravention of the proviso to sub-section (1).

38. Surveillance by the State

(1) No member of a competent organization 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 appropriate Surveillance and Interception Review Tribunal.

SAVE OUR PRIVACY

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

(3) An authorised officer seeking to carry out any surveillance of another person shall prefer an application, in such form and manner as may be prescribed by Central Government in consultation with the Privacy Commission, to the Surveillance and Interception Review Tribunal.

(4) The Surveillance and Interception Review Tribunal may, if it 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 cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.

(5) The Surveillance and Interception Review Tribunal may, if it 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 cognisable offence, for reasons to be recorded in writing addressed to the authorised officer, order the surveillance.

39. Surveillance by private persons or entities

(1) Notwithstanding anything contained in any other law for the time being in force, and without prejudice to the provisions of section 37 of this Act, no person who is not a member of a competent organization 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 her 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 by the Central Government in consultation with the Privacy Commission, members of the public of such surveillance.

40. Duration of surveillance

SAVE OUR PRIVACY

(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 Surveillance and Interception Review Tribunal, may, upon receipt of an application from an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, renew any order for surveillance if it is satisfied that the conditions upon which the original order was issued continue to exist.

Provided that where surveillance, under orders passed under this Chapter, including orders for renewal, has been carried out for a cumulative period of 6 months, whether in succession or not, any application for further renewal, shall be accepted, if in addition to the ground mentioned in this sub-section, the competent organization is able to demonstrate the need for such continued surveillance.

41. Duty to inform the person concerned

(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 or any surveillance carried out before this Act came into operation, the authorised officer who carried out the surveillance shall, in writing in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, notify, with reference to the relevant order of the Surveillance and Interception Review Tribunal, each person in respect of whom surveillance was carried out of the fact of such surveillance and duration thereof.

(2) The appropriate Surveillance and Interception Review Tribunal may, on an application made by an authorised officer in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, if it is satisfied that the

notification under sub-section (1) would 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 not be notified of the fact of such surveillance or the duration thereof:

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

42. Security and duty of confidentiality and secrecy

(1) Any person who carries out any surveillance, or who lawfully 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.

(2) 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.

(3) Every competent organization 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 ensuring that all surveillance carried out by the Competent Organization are in compliance with the provisions of this Chapter:

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 competent organization 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 ensuring that all surveillance carried out is in compliance with the provisions of this Chapter:

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

43. Disclosure of surveillance

(1) In addition to the existing obligations and duties for lawful, no person shall disclose to any person, other than the person who is being surveilled, 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 cognisable offence, that information, including personal data, obtained as a result of surveillance may be disclosed to an authorized officer of a competent organization 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.

44. Storage and destruction of surveillance

(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, and upon expiry of such period, shall destroy the data so stored.

SAVE OUR PRIVACY

(2) The appropriate Surveillance and Interception Review Tribunal may, on an application made in such form and manner as may be prescribed by the Central Government in consultation with the Privacy Commission, if it is satisfied that it is necessary to:

(i) prevent a reasonable threat to the security of the state; or

(ii) public order; or

(iii) prevent, investigate or prosecute a cognisable offence in an on-going legal proceeding and is authorized by a court order to that effect;

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 and shall not be destroyed.

(3) Any data obtained as a result of surveillance shall be stored in a manner that complies with the provisions of Section 14 with respect to such data.

45. Exception regarding reporting of violation of provisions of this Act

(1) Any communication, complaint, or evidence thereunder alleging violation of the provisions of this Act or other applicable law, if made to the Privacy Commission, the Surveillance and Interception Review Tribunals and their Public Advocates, or to the Supreme Court, shall not be treated as a violation of this Act and applicable provisions of the Information Technology Act, 2000.

CHAPTER V

SAVE OUR PRIVACY

THE PRIVACY COMMISSION

46. Constitution of the Privacy Commission

(1) The Central Government shall, by notification, issued within 6 months of the enactment of this Act, constitute, with immediate effect, a body to be called the Privacy Commission, by warrant under its hand and seal, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon it by or under this Act.

(2) The Privacy Commission shall be composed of at least three Privacy Commissioners, to be appointed by the President as specified by this Act.

(3) The Privacy Commission shall consist of two coordinate offices, namely the Office for Data Protection and the Office for Surveillance and Interception Reform, and such officers, other employees, and experts as may be appointed in accordance with the provisions of this Act.

(4) The Privacy Commission shall be autonomous, independent, and free from external interference. It shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers. Such powers shall be subject to audit by the Comptroller and Auditor General of India.

47. Appointment and Qualifications of Privacy Commissioners of Privacy Commission

(1) The Privacy Commission shall be composed of one Chief Privacy Commissioner and two or more than two Privacy Commissioners.

Provided that at least one Privacy Commissioner shall be a person who has been a Judge of the Supreme Court or has been a Chief Justice or Acting Chief Justice of a High Court.

SAVE OUR PRIVACY

Provided further that at least one or more Privacy Commissioner shall be a woman or a member of the third gender, or a transgender.

(2) The Chief Privacy Commissioner and the Privacy Commissioners shall be persons of outstanding ability, impeccable integrity and standing and who have special knowledge of, technical expertise in and professional or academic experience, of not less than 10 years cumulatively, in any one or more of the following domains

(i) Privacy law and policy;

(ii) Business and human rights;

(iii) Civil liberties;

(iv) Technology and ethics;

(v) Data collection, storage and protection practices, including emerging technologies.

(3) The Central Government shall issue a public advertisement inviting applications to fill all vacancies in the Privacy Commission. The selection committee for the appointment of the members of the Privacy Commission, shall be constituted by the Vice President of India and the selection panel shall comprise of the:

(i) Collegium of the Supreme Court of India,

(ii) the Law Minister,

(iii) the Leader of the Opposition from Lok Sabha or of the single largest Opposition party being one with the greatest numerical strength in the Lok Sabha,

SAVE OUR PRIVACY

(iv) Director of Indian Institute of Science,

(v) Director of an Indian Institute of Technology as appointed by the IIT Council,

(vi) one eminent person representing the private sector, and

(vii) one eminent person representing the civil society.

Explanation: 'Civil society' shall collectively mean 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.

(4) All proceedings of the selection committee shall be matters of public record and subject to pro-active disclosures under the Right to Information Act.

(5) No Members of Parliament or Members of the Legislature of any State or Union territory or a member of any political party shall be selected or appointed as a Chief Privacy Commissioner or Privacy Commissioner and persons holding any other office of profit or carrying on any business or practising any profession, before she enters upon this office, may be selected or appointed as Chief Privacy Commissioner or Privacy Commissioner, as the case may be, if –

(i) she holds any office of trust or profit, resigns from such office; or

(ii) she is carrying on any business, severs her connection with the conduct and management of such business; or

(iii) she is practising any profession, ceases to practise such profession.

SAVE OUR PRIVACY

48. Composition of the Office for Data Protection of the Privacy Commission

(1) The Office for Data Protection of the Privacy Commission shall be composed of a Director General of Data Protection, to be appointed by Privacy Commission through a notification, who shall be a person of standing, ability and integrity, qualified in law and with professional experience of not less than 5 years, cumulatively, in one or more of the following domains:

(i) investigation;

(ii) criminal procedure;

(iii) cybercrime and cyber forensics,

(iv) privacy and transparency law and policy.

(2) The number of other Additional, Joint, Deputy or Assistant Directors General or such officers or other employees in the Office of Data Protection, under the Director General, and the manner of their appointments, shall be such as may be prescribed by the Privacy Commission.

(3) Every Additional, Joint, Deputy and Assistant Directors General or such officers or other employees, shall exercise her powers, and discharge her functions, subject to the general control, supervision and direction or the Director General.

(4) The Additional, Joint, Deputy or Assistant Directors General or such officers of other employees, shall be appointed from amongst persons of integrity, ability and standing, and who have experience in law, investigation, public administration, economics and such other qualifications as may be prescribed by the Privacy Commission.

SAVE OUR PRIVACY

49. Composition of the Office for Surveillance and Interception Reform of the Privacy Commission

(1) The Office for Surveillance and Interception Reform of the Privacy Commission shall be composed of a Director General of Surveillance and Interception Reform, to be appointed by the Privacy Commission through a notification, who shall be a person of ability, integrity and standing, qualified in law and with professional experience of not less than 5 years, cumulatively, in any or more of the following domains:

(i) civil liberties,

(ii) criminal procedure,

(iii) governmental oversight,

(iv) transparency,

(v) police reforms.

(2) The number of other Additional, Joint, Deputy or Assistant Directors General or such officers or other employees in the Office of Data Protection, under the Director General, and the manner of their appointments, shall be such as may be prescribed by the Privacy Commission.

(3) The number of other Additional, Joint, Deputy or Assistant Directors General or such officers or other employees in the Office of Data Protection, under the Director General, and the manner of their appointments, shall be such as may be prescribed by the Privacy Commission.

(4) Every Additional, Joint, Deputy and Assistant Directors General or such officers or other employees, shall exercise her powers, and discharge her functions, subject to the general control, supervision and direction or the Director General.

(5) The Additional, Joint, Deputy or Assistant Directors General or such officers of other employees, shall be appointed from amongst persons of integrity, ability and standing, and who have experience in law, investigation, public administration, economics and such other qualifications as may be prescribed by the Privacy Commission.

50. Officers and other employees of the Privacy Commission

(1) The Commission may appoint such officers and other employees as it considers necessary for the efficient performance of its functions under this Act.The Commission may engage such number of experts and professionals of integrity and outstanding ability, who have special knowledge of, and experience in, data, transparency, information, law, technology, economics or such other disciplines related to privacy, as it deems necessary to assist the Commission in the discharge of its functions under this Act.

(2) The salaries and allowances payable to and other terms and conditions of service of the officers and other employees of the Commission and the number of such officers and other employees shall be such as may be prescribed by the Privacy Commission.

(3) The Commission may engage such number of experts and professionals of integrity and outstanding ability, who have special knowledge of, and experience in, data, transparency, information, law, technology, economics or such other disciplines related to privacy, as it deems necessary to assist the Commission in the discharge of its functions under this Act.

51. Term of office, conditions of service, etc. of Privacy Commissioners and Offices constituted under the Commission

SAVE OUR PRIVACY

(1) Before appointing any person as a Chief Privacy Commissioner or Privacy Commissioner, the President shall satisfy herself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially their functions as such Chief Privacy Commissioner or Privacy Commissioner.

(2) The Chief Privacy Commissioners 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, but shall be eligible for reappointment:

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

Provided further that no person shall hold office as a Chief Privacy Commissioner or Privacy Commissioner after they have attained the age of 75 years.

(3) Notwithstanding anything contained in sub-section (2), a Chief Privacy Commissioner or any Privacy Commissioner may –

(i) by writing under her hand and addressed to the President resign her office at any time;

(ii) be removed from office in accordance with the provisions of Section 43 of this Act.

(4) A vacancy caused by the resignation or removal of a 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 a Chief Privacy Commissioner, such one of the Privacy Commissioners as the President may, on the advice of the selection committee under Section 47 (3), by notification, authorise in this behalf, shall act as the Chief Privacy Commissioner till the date on which a new Chief Privacy

Commissioner, appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

(6) When a 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 a Chief Privacy Commissioner and Privacy Commissioners shall be such as may be prescribed by the Central Government:

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

(8) The salaries and allowances payable to and the other terms and conditions of service of the Director General of Data Protection, the Director General of Surveillance, any Additional, Joint, Deputy or Assistant Director General, Secretary, officer, employee appointed or expert or professional engaged shall be such as may be prescribed by the Privacy Commission.

(9) The Chief Privacy Commissioners 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.

52. Removal of Chief Privacy Commissioners and Privacy Commissioners

(1) The President may remove from office the Chief Privacy Commissioner or any Privacy Commissioner, who –

SAVE OUR PRIVACY

(i) is adjudged an insolvent; or

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

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

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

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

(vi) has acquired such financial or other interest as is likely to affect prejudicially her 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

(vii) 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 a 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.

53. Functions of the Privacy Commission

(1) The Privacy Commission may, through decisions arrived at by a simple majority of its members present and voting as set out in Section 58(1) of this Act, authorize, review,

investigate, make an inquiry, and/or monitor, suo motu or on a petition presented to it by any person, group of persons or by someone acting on his or their 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 of the following functions, namely –

(i) 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;

(ii) review and/or monitor any measures taken by any competent organization, company, person or other entity for the protection of privacy and take such further action as it deems fit;

(iii) authorize, review and/or monitor any action, code, certification, policy or procedure of any competent organisation, company, person or other entity to ensure compliance with this Act and any rules made hereunder;

(iv) enforce the provisions of this Act at its own instance or on the basis of complaints received by it, through means including the issuance of appropriate orders and directions, the pursuit of binding settlements with offending persons and the levy of fines;

(v) formulate, through transparent, inclusive and pervasive public consultations with experts, other stakeholders, and the general public, norms and rules for the effective protection of privacy by competent organisations, companies, persons or other entities;

SAVE OUR PRIVACY

(vi) 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; and

undertaking training and knowledge building for data controllers, including those involved in the provision of essential services and law enforcement;

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

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

(ix) ensure the speedy and efficient redressal of all complaints, whether made by a lone data subject or a group of them or on their behalf, whose cause of action arises from this Act;

(x) undertake efforts to facilitate international co-operation with regards to data protection, and allied subjects, including enforcement;

(xi) advise the Central Government on the grant of adequacy status in respect of cross border data flows;

(xii) coordinate in writing across State Privacy Commissions, State Governments and regulatory bodies including the Bureau of Indian Standards which may also be concerned with data protection in order to harmonize and classify standards for data including open data sets which contain personal data;

SAVE OUR PRIVACY

(xiii) Such other functions as it may consider necessary for the protection of privacy, personal data, the prevention of the abuse of the criminal process, both investigatory and judicial, by the State, and enforcement of this Act;

(xiv) Publish periodic reports providing description of performance, findings, conclusions or recommendations of any or all of the functions assigned to the Privacy Commission in this Chapter.

(3) Without prejudice to the generality of the foregoing provision, the Office of Data Protection within the Privacy Commission shall perform all of the following functions, namely:

(i) Investigate data controllers and processors, whether initiated on complaint of a data subject or a group of them or on their behalf or on direction of the Privacy Commission or suo motu, for the purpose of identifying activities which are in contravention of the provisions of this Act, either at its own instance or upon receipt of credible information or complaint;

(ii) Obtain from the data controllers and processors, access to all personal data and to all information necessary for the performance of its tasks.

(iii) publish and make publicly available periodic reports concerning the incidence of compliance including violations of this Act and data breaches as reported under this Act;

(iv) assist Privacy Commission in policy formulation and other activities for effective protection of privacy;

(v) coordinate with the Office for Surveillance and Interception Reform in such manner as is necessary or may be useful to the achievement of the purposes of this Act;

SAVE OUR PRIVACY

(4) Without prejudice to the generality of the foregoing provision, the Office for Surveillance and Interception Reform in the Privacy Commission shall perform all of the following functions, namely;

(i) assist Privacy Commission in formulation of policy and other activities for bringing about reforms in carrying out interception and surveillance by competent organization, companies, persons or other entities;

(ii) collection of data from competent organizations on interception and surveillance carried out by those and analyze the same for the purpose of preparing periodic reports on compliance with provisions of this Act, including comprehensive data concerning violations of the processes of interception of communications and surveillance;

(iii) advise on appointments of public advocates, as provided under subsection (4) of section 68, for the purpose of defending the person being surveilled or intercepted before the Surveillance and Interception Review Tribunal;

(iv) to appear before a Surveillance and Interception Review Tribunals to provide expert evidence and testimony;

(v) ensure the speedy and efficient redressal of all complaints, whether made by a lone data subject of a group of them or in their behalf, whose cause of action arises from this Act;

(vi) coordinate with the Office of Data Protection in such manner as is necessary or may be useful to the achievement of the purposes of this Act;

(5) The Periodic Reports published by the Privacy Commission, stipulated in sections 53(2)(n) and 53(3)(c), shall be tabled before both Houses of Parliament during the Parliamentary

Session that succeeds the publication of any Periodic Report and the same shall be made publicly available, immediately thereafter.

(6) The Chief Privacy Commissioners, Privacy Commissioners and Directors General shall appear before a special ad hoc Committee, constituted by the Speaker of the Lok Sabha and comprising of members from both the governing and the opposition parties from both houses of Parliament, on a quarterly basis. The ad hoc Committee shall -

(i) be empowered to review the functioning of the Privacy Commission, and may ask the Chief Privacy Commissioners and the Privacy Commissioners any questions in this regard, as per procedure of the functioning of the Committee.

(ii) prepare and present periodic reports to both houses of Parliament in a manner regulated by the Committee.

(iii) all hearings of the ad hoc committee will be held in public with regard to the principles of transparency and wide, inclusive participation.

(7) 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, judgment, decree or order made by it.

(8) 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.

(9) The Privacy Commission may, in its own name, sue or be sued.

54. Salaries, etc. to be defrayed out of the Consolidated Fund of India

(1) The salaries and allowances payable to the Chief Privacy Commissioners, Privacy Commissioners, Director Generals, any Additional, Joint, Deputy or Assistant Director

SAVE OUR PRIVACY

General, Secretary, officer, employee appointed or expert or professionals engaged and the administrative expenses of the Privacy Commission shall be defrayed out of the Consolidated Fund of India.

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

(1) No act or proceeding 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.

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

(1) The Chief Privacy Commissioners and Privacy Commissioners and other employees of the Privacy Commission shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

57. Location of the Privacy Commission

(1) The Privacy Commission shall be located in New Delhi or in such other location as directed by the Chief Privacy Commissioner in consultation with the Central Government.

58. Jurisdiction of the Privacy Commission

(1) Investigations or actions for enforcement may be instituted in the Privacy Commission, suo motu or on complaints made by any person, group of persons or anyone on their behalf, in respect of cases involving–

(i) data collection or processing by or on behalf of the Central Government;

SAVE OUR PRIVACY

(ii) a conflict between two State Privacy Commissions; or

(iii) extraterritorial transfers of data pertaining to Indian data subjects.

(2) Any disputes as to jurisdiction shall be resolved in a manner that would accord the data subject the most timely and cost-effective access to redress, or promote the most timely and cost effective enforcement of the provisions of this Act.

59. Procedure to be followed by the Privacy Commission

(1) Subject to the provisions of this Act, the Privacy Commission, in coordination with both Offices constituted under it, shall have power to make rules to prescribe –

(i) the procedure and conduct of its business;

(ii) the delegation to one or more Privacy Commissioners of such powers or functions as the Privacy Commission 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 crosser-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.

(3) Nothing in this section shall prevent either Office in the Privacy Commission from making rules in respect of matters of procedure exclusively concerning it.

60. Power relating to inquiries

SAVE OUR
PRIVACY

(1) The Privacy Commission, including offices constituted under it, shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –

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

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

(iii) the reception of evidence on affidavit;

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

(v) the issuing of any commission for the examination of witnesses; and,

(vi) any other matter which may be prescribed by the Central Government.

(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 section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

(3) he Privacy Commission or any other officer, not below the rank of a Gazette Officer, specially authorized 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 there from subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), 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 (45 of 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 (2 of 1974), 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 (2 of 1974).

61. Decisions of the Privacy Commission

(1) The decisions of the Privacy Commission shall be taken by majority 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 has the power to:

(i) require a competent organisation, company, person or other entity to take such steps as may be necessary to secure compliance with the provisions of this Act;

(ii) require a competent organisation, company, person or other entity to compensate any person for any loss or detriment suffered;

(iii) impose penalties.

62. Proceedings before the Privacy Commission to be judicial proceedings

SAVE OUR PRIVACY

(1) 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 (2 of 1974), 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 (45 of 1860).

63. Appeals

(1) Subject to any conditions prescribed by rules made in this regard by the Central Government, in consultation with the Attorney General of India and the Chief Justice of India, all appeals from Privacy Commission shall lie to a bench of the Supreme Court, specifically designated by the Chief Justice of India in that regard.

CHAPTER VI

STATE PRIVACY COMMISSIONS

64. State Privacy Commissions

(1) Every State Government shall, within a year of the enactment of this Act, by notification in the Official Gazette, with immediate effect, constitute a body to be known as the (name of the State) Privacy Commission to exercise the powers conferred on, and to perform the functions assigned to, it under this Act.

(2) Every State Privacy Commission shall consist of at least one Privacy Commissioner, to be appointed by the Governor of that State

(3) Every State Government shall issue a public advertisement inviting applications to fill all vacancies in the State Privacy Commission. The selection committee for the appointment of

the members of the State Privacy Commission shall be constituted by the Governor of that State and shall comprise of the:

(i) Chief Justice and two senior most judges of the State High Court,

(ii) the Law Minister of the State Government,

(iii) the Leader of the Opposition from Vidhan Sabha or of the single largest Opposition party being one with the greatest numerical strength in the Vidhan Sabha,

(iv) one eminent person with experience in technology and academic or public interest research,

(v) representing the private sector, and

(vi) one eminent person representing the civil society.

All proceedings of the selection committee shall be matters of public record.

Explanation: 'Civil society' shall collectively mean non-governmental and non-profit organisations that perform activities for the general upliftment and interests of the people in the field privacy and is independent of government funding, interference or influence.

(4) No Members of Parliament or Members of the Legislature of any State or Union territory or a member of any political party shall be selected or appointed as a State Privacy Commissioner and persons holding any other office of profit or carrying on any business or practicing any profession, before she enters upon this office, may be selected or appointed as State Privacy Commissioner, as the case may be, if –

(i) she holds any office of trust or profit, resigns from such office; or

(ii) she is carrying on any business, severs her connection with the conduct and management of such business; or

(iii) she is practicing any profession, ceases to practice such profession.

(5) Except as provided for expressly under this Act, a State Privacy Commission shall have powers and functions coequal and identical to those of the Privacy Commission in all respects.

(6) A State Privacy Commission may appoint such officers and other employees, or engage any professional or expert, as it considers necessary for the efficient performance of its functions under this Act.

(7) Every State Privacy Commission shall be autonomous, independent, and free from external interference. It shall be provided with sufficient operational resources including human, technical, and financial for the effective discharge of its duties and exercise of its powers. Such powers shall be subject to audit by the Comptroller and Auditor General of India.

(8) The salaries and allowances payable to and the other terms and conditions of service of State Privacy Commissioners shall be such as may be prescribed by the State Government.

(9) The salaries and allowances payable to and the other terms and conditions of service of any officer, employee appointed or expert or professional engaged shall be such as may be prescribed by the State Privacy Commission.

65. Jurisdiction of the State Privacy Commissions

(1) Investigations or actions for enforcement may be instituted in the State Privacy Commission, suo motu or on complaints made by, any person, group of persons or anyone on their behalf, within the local limits of whose jurisdiction –

(i) the complainant or data subject actually and voluntarily resides;

(ii) where the data controller or data processor is physically located or principally carries out business; or

(iii) the cause of action, wholly or in part, arises.

(2) Any disputes as to jurisdiction shall be resolved in a manner that would accord the data subject the most timely and cost-effective access to redress, or promote the most timely and cost effective enforcement of the provisions of this Act.

66. Appeals

(1) Subject to any conditions prescribed by rules made in this regard by appropriate State Government, all appeals from a State Privacy Commission shall lie to a bench of the respective High Court, specifically designated by the Chief Justice in that regard.

(2) Notwithstanding sub-section (1), appeals from a State Privacy Commission shall lie to the Privacy Commission where -

(i) there is a dispute as to jurisdiction between two or more State Privacy Commissions; or

(ii) two or more State Privacy Commissions have passed orders or directions, or otherwise taken any action in respect of the same cause of action

Provided that in any such appeal, the Privacy Commission shall be included as a necessary party.

67. Procedure

SAVE OUR PRIVACY

(1) The State Government shall, in consultation with its Advocate General, the Chief Justice of its High Court and the Privacy Commission, prescribe rules governing the procedures to be followed:

(i) by and before the State Privacy Commission, and

(ii) in respect of appeals to its High Court in terms of sub-section (1) of Section 66 of this Act.

68. Power to make rules

(1) Subject to the provisions of this Act, every State Government may, in consultation with the State Privacy Commission, by notification in the Official Gazette, prescribe rules in order to bring into effect any of the provisions of this Chapter of the Act.

CHAPTER VII

SURVEILLANCE AND INTERCEPTION REVIEW TRIBUNALS

69. Surveillance and Interception Review Tribunals

(1) The Central Government shall, by notification in the Official Gazette, constitute, within a period of 6 months from the enactment of this Act, a Tribunal in every High Court to be known as the "Surveillance and Interception Review Tribunal", hereinafter referred to as the Tribunal.

Provided that if the Tribunal is not constituted within the stipulated time period, no order for interception or surveillance issued after a period of 90 days from the date the stipulated time period for constitution of the Tribunal gets over, shall be valid and any

SAVE OUR PRIVACY

interception or surveillance carried out under such an order shall be a violation of the provisions of this Act.

Provided further that if the Tribunal is not constituted within the stipulated time period and till the time it is constituted, no existing order of surveillance or interception can be renewed.

(2) The Central Government shall appoint, for a period of two years or till the retirement of the Judge so appointed, whichever is earlier, two or more Judges of the High Court, as publicly designated by the Chief Justice of that High Court in consultation with the appropriate State Government, as the Tribunal

(3) The Central Government shall make available to the Tribunal such stag as may be necessary for the discharge of its functions under this Act.

(4) Subject to the provisions of this Act, one or more Public Advocates, shall be appointed by the Chief Justice of the High Court of that State, in consultation with the Office for Surveillance and Interception Reform of the Privacy Commission, the respective State Privacy Commission, the State Legal Services Authority, and the Bar Council of that State, for the purpose of defending the interest of the person being surveilled or intercepted, ensuring compliance with the provisions of this Act, and advancing legal arguments that further the protection of privacy and other fundamental rights under the Constitution

Provided that:

In appointing one or more Public Advocates, the Chief Justice of the High Court of the State will do so after issuing public notice inviting applications of interest; and

(i) A person shall be qualified to be appointed a Public Advocate to the Tribunal if she is;

SAVE OUR PRIVACY

(ii) A citizen of India, qualified to practice law with at least 7 years' experience at the bar; and

(iii) Has experience with litigation on fundamental rights, criminal law and procedure, policing powers and oversight, and communications and information technology laws;

(5) Once appointed, any Public Advocate shall:

(i) be provided copies of all ordinary applications made to and government orders shared with the Tribunal under this Act, including their supporting documents and flings;

(ii) have a right of attend, be heard, and to file briefs and other flings before all proceedings of the Tribunal; and

(iii) be empowered to file appeals with respect to orders of the Tribunal to the Supreme Court as provided for under this Act.

Provided that any decisions not to file an appeal shall be made only after a legal opinion on the merits of the case and the decision for reasons recorded in writing which shall be made available alongwith the complete case files including all pleadings and materials when the disclosure of the orders of the Surveillance and Interception Review Tribunal are made as per the provisions under the act.

(6) All expenses incurred in connection with the Tribunal shall be defrayed out of the Consolidated Fund of India.

(7) Subject to any Rules made in this regard by the Central Government, in consultation with the Privacy Commission, the Tribunal shall have power to regulate its own procedure in all matters arising out of the discharge of its functions including.

SAVE OUR
PRIVACY

Explanation- Such Rules may provide for inner-camera proceedings of the Tribunal, the manner in which third parties interested in the matter may make application for attending the hearings before the Tribunal, for making the decisions of the Tribunal public after a stipulated time period not exceeding one year since the date of the order and other incidental matters.

(8) The Tribunal shall, for the purpose of making an inquiry under this Act, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit, in respect of the following matters, namely:—

(i) the summoning and enforcing the attendance of any witness and examining him on oath;

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

(iii) the reception of evidence on affidavits;

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

(v) the issuing of any commission for the examination of witnesses.

(9) Any proceeding before the Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 of the Indian Penal Code (45 of 1860) and the Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code.

(10) Subject to provisions of this Act, the Director General of Surveillance and Interception Reform constituted under the Privacy Commission, shall have access to the proceedings of the Tribunal in order to assist the Tribunal by providing expert evidence, legal arguments, and testimony.

SAVE OUR PRIVACY

70. Appointment, terms of service, etc

(1) Terms of service, removal and allied matters relating to persons appointed to the Tribunal shall be governed by rules made in this regard by the Central Government, in consultation with Privacy Commission and appropriate State Government.

Provided that no terms and conditions of service of persons appointed to the Tribunal shall be varied to their disadvantage after their appointment.

71. Jurisdiction of the Surveillance and Interception Tribunals

(1) Subject to the provisions of Chapter IV of this Act, the Tribunal, which shall review, renew or take any other action with respect to orders of surveillance or interception, shall be the Tribunal within the local limits of whose jurisdiction –

(i) the person to be surveilled or intercepted actually and voluntarily resides;

(ii) where the competent organization seeking to undertake surveillance or interception is physically located; or

(iii) where the actual act of interception or surveillance is to be carried out.

72. Appeals

(1) Subject to any conditions prescribed by rules made in this regard by the Central Government, in consultation with the Privacy Commission, and the appropriate State Governments, all appeals from any of the Tribunals shall lie to a bench of the Supreme Court, specifically designated by the Chief Justice of India in that regard

SAVE OUR PRIVACY

CHAPTER IX

OFFENCES AND PENALTIES

73. Punishment for offences related to personal data

(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 1 crore rupees.

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

Provided further that in case of companies, the penalty shall be governed by Section 77.

(2) Whoever attempts to commit any offence under sub section (1) shall be liable in the manner and to the extent provided for such offence under that sub-section.

(3) 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 to 10 crore rupees.

Provided that whoever commits the offence defined above 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.

Provided further that in case of companies, the penalty shall be governed by Section 77.

(4) Whoever attempts to commit any offence under sub section (3) shall be punishable with the punishment provided for such offence under that sub-section.

SAVE OUR PRIVACY

74. Punishment for offences related to interception of communication

(1) 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 to 1 crore rupees.

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

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

75. Punishment for offences related to surveillance

(1) 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 10 crore rupees.

Provided that whoever commits the offence defined above 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.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub section.

76. Abetment and repeat offenders

(1) 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.

SAVE OUR PRIVACY

77. Offences by companies

(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.

78. Cognisance

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offences under this chapter shall be cognisable and non-bailable.

79. General penalty for failure to comply with notice or order issued under this Act

(1) 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 1 crore rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend to 10 lakh

rupees for every day after the first during which he has persisted in such failure or contravention.

80. Punishment to be without prejudice to any other action

(1) 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

81. Power to make rules

(1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act till such time as the Privacy Commission is set up.

(2) The Privacy Commission may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

Provided that where the Privacy Commission makes rules upon a subject already covered by the Central Government, it shall ensure that protections accorded to data subjects by its rules are maintained or improved.

(3) In particular, and without prejudice to the generality of the foregoing powers, such rules may provide for such measures as may be necessary to secure -

(i) all personal data related to data subjects located in India; and

SAVE OUR PRIVACY

(ii) any personal data flowing into and out of, exported or imported out of India.

(iii) the notification of theft, loss or damage under sub-section (4) of section 16;

(iv) the notification of disclosure under sub-section (5) of section 18;

(v) the application by an intelligence organisation under sub-section (1) of section 30;

(vi) the application to intercept a communication under sub-section (1) of section 29;

(vii) the application to renew an interception of communication under sub-section (2) of section 32;

(viii) the notification of an interception of communication under sub-section (1) of section 33;

(ix) the application to not inform under sub-section (2) of section 33;

(x) the application to store information obtained as a result of any interception of communication under sub-section (2) of section 36;

(xi) the application to carry out surveillance under sub-section (3) of section 38;

(xii) notification to the general public under sub-section (2) of section 39;the application to renew surveillance under sub-section (2) of section 40;

(xiii) the notification of surveillance under sub-section (1) of section 41;

(xiv) the application to not inform under sub-section (2) of section 41;

SAVE OUR PRIVACY

(xv) the application to store information obtained as a result of surveillance under sub-section (2) of section 44;

(xvi) 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;

(xvii) procedure to be followed by the Privacy Commission;

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

(xix) the effective implementation of this Act.

(4) 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 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.

(5) Every rule made by the Central Government under sub-section (1) shall require express assent of Parliament.

Provided that where such assent is not obtained, the rules will be *void ab initio*.

82. Bar of jurisdiction

SAVE OUR PRIVACY

(1) On and from the appointed day, courts or authorities shall have, or be entitled to exercise jurisdiction with respect to remedies provided for Data Subjects and against Data Subjects under this Act with respect.

Provided that legal proceedings for reliefs in the nature of interim injunctions or mandatory injunctions shall not be initiated against the authorities provided for under this act including but not limited to the State Privacy Commission and the Privacy Commission.

Provided that further provisions of the Arbitration and Conciliation Act, 1996 shall not bar the Privacy Commission or the State Privacy Commission or any other body from exercising jurisdiction under the provisions of this Act.

(2) No order passed under this Act shall be appealable except as provided therein and no injunction shall be granted by any court or tribunal to any authority established under this Act in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

83. Protection of action taken in good faith

(1) 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.

(2) Notwithstanding anything inconsistent therewith contained in any other law for the time being in force any communication or complaint made in good faith made by any person alleging violation of the provisions of this act, if made to the Privacy Commission, the

SAVE OUR PRIVACY

Surveillance and Interception Review Tribunals and their Public Advocates, or to any High Court or the Supreme Court, shall not be treated as a violation of this Act or any other law.

84. Power to remove difficulties

(1) If difficulty arises in giving effect to the provisions of this Act as provided for under this section, 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) The provisions of sub-section (1) shall only apply in instances when it is with respect to conflict between this Act and any existing law;

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

85. Act to have overriding effect

(1) Except as otherwise provided in 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, including provisions in -

(i) Sections 43A, 69, 69B, 72 and 72A of the Information Technology Act, 2000; and

(ii) Sections 7, 28, 29, 30, 31, 32, 33 and 47 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016; and

(iii) Section 5(2) of the Indian Telegraph Act, 1885; and

SAVE OUR PRIVACY

(iv) Section 21 of the Prevention of Money Laundering Act, 2002; and

(v) The Census Act, 1948.

(2) Nothing contained in sub-section (1) shall apply to the provisions of the Representation of the People Act, 1951 and the Right to Information Act, 2005.