SECRET

No. II/20034/250/2011-IS-II
Government of India
Ministry of Home Affairs
IS-I Div (IS-II Desk)

North Block, New Delhi,
Dated 29th Sept' 2011

OFFICE MEMORANDUM

Subject: Draft Bill on Right to Privacy.

The undersigned is directed to say that Union Home Secretary will take a meeting at 2.30 PM on 7-10-2011 (Friday) in his Chamber, North Block, New Delhi to discuss the draft bill on Right to Privacy – in particular the issues arising from the discussion held in CoS held on 27-5-2011 and the opinion of the Ld Attorney General.

2. It is requested to kindly make it convenient to attend the above mentioned meeting.

3. A copy of the proposed discussion points is enclosed.

29/09
(U S P Kushwaha)
Dy Secretary (IS-I)

1. DoT
(Shri R Chandrasekhar, Secretary),
Sanchar Bhawan, New Delhi

2. DoPT
(Ms Alka Sirohi, Secretary),
North Block, New Delhi.

3. Intelligence Bureau,
(Shri N Sandhu Director),
SP Marg, New Delhi.

For brief
cc to: AS(T)
OSD to Secy(IT)

Copy to:-

1. PPS to HS
2. PS to JS (IS-I)
3. PS to Director (IS-I)

Secretary (T) desired me to attend the meeting. Kindly get background papers * from DDG (PG)

4/10/11

As desired by OSD to Secy(T), the papers are being sent to DDG (Security) for attending

SECRET

Discussion Points for the Meeting to be taken by Home Secretary at 2.30 PM on 7-10-2011 to discuss Draft Privacy Bill

Upon the DoPT's draft Bill on Right to Privacy, Ld Attorney General opined that conditions under which interception of communication could be permitted should be spelt out in chapter IV of the Bill itself rather than making a reference to other sections. He also suggested that provisions about authorization of interception of communications (web/IT based communications) should be so drafted that it may have overriding effect over similar provisions in Telegraph Act, IT Act or any other Act. It was agreed that procedure for grant of authorization etc would be left to the rule making power of the Govt. The Ld Attorney General also opined that the Rules should be drafted simultaneously and suggested that while drafting the Rules, recommendations of Chandrasekhar Committee and instructions and guidelines issued by Ministry of Home Affairs should be kept in view. The Attorney General also suggested redrafting of Chapter V of the Bill which relates to surveillance.

2. The following are the legal/practical issues which flow from opinion of Ld Attorney General and which require consideration:-

(a) Difficulty of consolidating in a coherent manner the various scattered and relatable provisions & rules (IT Act/Telegraph Act/Wireless Act being the primary legislation, apart from provisions of CrPC etc) into the proposed Privacy Act.

(b) Further, all "amendments" to the lawful interception regime would thus become Privacy Law issues. Presently, IT Act in its totality is led by DIT & Telegraph & Wireless Act by DoT. Given that L.I provisions are deeply embedded in technical/technology issues – such a relocation (as suggested by Ld AG) would present serious domain management issues.

(c) Both, as a principle of legislative drafting & for clarity – simpler construct would be that the proposed Privacy law accounts for the lawful interception regime, as it exists, as an permissible "exception" to the Privacy Law.

SECRET

No. 501/2/6/2011-CA.V
CABINET SECRETARIAT
RASHTRAPATI BHAWAN

Subject: **Draft Bill on the Right to Privacy.**

A meeting of Committee of Secretaries (CoS) was held under the Chairmanship of the Cabinet Secretary on 27th May, 2011 at 3.30 p.m. in Committee Room of the Cabinet Secretariat to consider a CoS proposal received from Ministry of Personnel, Public Grievances and Pensions (MoPPG&P), Department of Personnel and Training (DoPT) vide their Note No. 17/2/2010-IR, dated 24.4.2011 regarding Draft Bill on the Right to Privacy.

2. Joint Secretary (AT&A), DoPT, made a brief presentation on the draft "Right to Privacy Bill" before the CoS. There was broad agreement that there should be a comprehensive legislation on Privacy. It was also agreed that the particular structure of the draft bill presented for discussion may be retained, but several provisions need to be re-arranged and/or elaborated in order to ensure that the legislation becomes comprehensive and references to other legislations are minimized. The discussions on specific issues of the draft Bill along with the decisions taken thereon are as follows:

I. **Object Clause:** It was felt that object clause does not do full justice to the Bill as it focuses primarily on data protection. It was also stated that the object clause should be drafted carefully as interpretation of the Act is often made with reference to the object clause. It was, therefore, decided that the object clause would be re-drafted highlighting the Government's intention to provide all individuals, through legislation, the right to privacy; to detail the actions needed to be taken by the State and private persons to respect this right; and, specify the circumstances under which restrictions may be placed on the exercise of this right.

II. **Applicability:** It was decided that since Article 21 of the Constitution is applicable to all individuals, the right to privacy bill should also extend to all individuals, whether citizens are not.

III. **Chapter-II of the draft Bill:** It was decided that Section 3 needs to be re-drafted. It is important to ensure that the law states upfront, that all individuals have a right to privacy. It is also important to define the contours of this right clearly in the legislation. Thereafter, in another section, those circumstances may be detailed when reasonable restrictions may be put on the operation of these rights.

IV. It was also decided that the reference in **Section 4** to non-application of the Act in the case of journalistic publications need not be included. The Ld Attorney General also opined that a general exemption to disclosure made under RTI Act may not be appropriate as some of the provisions under the RTI Act (which provide for protection of privacy of individuals) need re-drafting in the context of recent experience with the Act.

V. **Chapter-III:** There was broad agreement on the structure and content of various provisions regarding data privacy as laid down in Chapter III. However, Secretary, Department of Information Technology (DoIT), pointed out that some rules have recently been notified under the Information

Technology Act and it should be ensured that there is no inconsistency between those rules and the provisions as set out in this bill regarding collection and processing of data etc.

VI. In regard to **Section 12** which deals with sensitive personal data, it was pointed out that certain provisions need to be reviewed. For example, insurance companies should be able to access medical data/health data of the individual, and employers may also need access to the banking/financial data of the individual.

A query was made regarding applicability of these provisions in regard to investigations and offences and also whether sharing of data among Government Departments would be possible. It was clarified that exemptions have been provided in Section 19 of the Bill which covers data collection for the purposes of investigation of offences etc. As regards sharing of data amongst Government Departments, this issue would be examined in more depth and the relevant provision would be re-drafted.

VII. **Chapter-IV:** The Ld. Attorney General was of the view that this chapter needs to be strengthened by including detailed provisions regarding the circumstances, in which communication may be intercepted, the authority which will permit such interception and related matters. This is all the more important as the current provisions of the Indian Telegraph Act (Section 5(2)) are weak and outdated. Further, agencies which can do interception may also be listed in a schedule annexed to the Act.

It was clarified by JS(AT&A) that a detailed definition of 'interception of communication' been provided in the bill and to this extent, the weakness of Section 5(2) of IT Act has been addressed. It was also mentioned that interception of communication is also made under Prevention of Terrorism Act 2002 and IT Act 2000 and therefore, it should be considered whether all interceptions (telephone, internet etc.) should be governed by same set of provisions or should the provisions contained in legislations mentioned above co-exist as long as they satisfy the basic principles, as laid down in the bill.

VIII. It was decided that **Chapter IV** needs to be further strengthened and redrafted so that detailed methodology for all interceptions is laid down in this Act itself.

IX. **Chapter-V:** While there was agreement that there should be provisions regarding CCTV and other surveillance in the Bill, it was agreed that right to privacy may not be available in case of images captured in a public place as the concerned individual is aware that he is in a public place and should not expect privacy in such circumstances. As regards surveillance, it was noted that the current provisions are inadequate and detailed legal provisions may be drafted in this Act itself to control all surveillance.

Secretary to Prime Minister pointed out that it should be ensured that surveillance made by intelligence agencies for the purpose of security of state may not be hampered because of such provisions. The Ld. Attorney General was also of this view that security of state would always prevail over right to privacy of the individual and this needs to be ensured. JS(AT &A) clarified that even in this draft, such intelligence gathering has been exempted and assured that this would be ensured while redrafting the Bill.

X. **Chapter-VI:** There was agreement that strong legal provisions need to be made for checking unsolicited commercial communication.

XI. **Chapter-VII:** While constitution of a body to aid and advise the government in regard to data privacy issue was accepted 'in principle', it was suggested that this body may be renamed as an Advisory Council considering that its functions are mainly in the realm of advising the government on data privacy issue and finalizing codes of practice etc.

XII. **Chapter-VIII:** There were no significant observations made in the meeting regarding provision of Chapter VIII which deal with grants, funds, accounts and audit etc of the Data Protection Authority.

XIII. **Chapter-IX:** It was agreed that Cyber Tribunal set up under IT Act may be designated as Appellate Tribunal for the purpose of this bill, as proposed.

XIV. **Chapter-X:** Individual sections were not discussed. It was felt that once changes are made in the bill as discussed in the meeting, provision of this chapter should also be reviewed to ensure consistency.

XV. Learned Attorney General observed that the non-obstante provisions of Section 5 (that in case of any conflict between this Act and other legislations with regard to privacy provisions, provision of this Act shall prevail) should find a place in **Chapter XI** rather than in Chapter II, as is currently proposed.

3. Cabinet Secretary desired that the bill may be redrafted keeping above observations in view. He requested Ld. Attorney General to guide the department in re-drafting, particularly in regard to how detailed provisions regarding interception and surveillance etc. need to be incorporated within this legislation.

4. After detailed deliberations it was decided that DoPT will redraft the Bill in the light of the observation made in the above paragraphs. The Bill may be reconsidered by Committee of Secretaries and thereafter, before it is finalized, it should be placed in public domain for comments / suggestions.

~~~~~~~~
~~~~~~~~

THE RIGHT TO PRIVACY BILL, 2011

A Bill to provide for the right to privacy to citizens of India and regulate the collection, maintenance, use, and dissemination of their personal information and provide for penal action for violation of such right and for matters connected therewith or incidental thereto.

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

Chapter - I : Preliminary

1. **Short title, extent and commencement**

(1) This Act may be called the Right to Privacy Act, 2011.

(2) It extends to the whole of India (except Jammu and Kashmir).

(3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act.

2. **Definitions**

In this Act, unless the context otherwise requires –

(i) "Anonymised" means in relation to personal data, the deletion of all information that:

(a) identifies the data subject; or

(b) can be used to identify the data subject by linking to any other information that identifies the data subject.

(ii) "Appellate Tribunal" means the Cyber Appellate Tribunal established under sub-section (1) of section 48 of the Information Technology Act, 2000;

(iii) "Authority" means the Data Protection Authority of India established under sub-section (1) of section 33;

(iv) "Chairperson" means the Chairperson of the Authority appointed under sub-section (3) of section 33;

(v) "Collection of personal data" means collection, received, recording or retrieval by any means.

(vi) "Communication" means a process of sharing facts, ideas, opinions, thoughts and information through speech, writing, gestures, sound,

images, signals or pictures, graphs, symbols, diagrams between two or more individuals through telephonic conversations, radio message, electronic mode(including internet or satellite) or postal letters or any other mode and "**Unsolicited Commercial Communication**" means any commercial communication which a data subject has not opted to receive but excludes any message transmitted on the directions of the central government, the state government or any agencies authorized by them.

(vii) "Communication Data" means any data that identifies the usage of any postal or telegraphic service by an individual but does not include the contents of such communication.

(viii) "Consent" includes implied consent.

(ix) "Data Controller" means any person who processes personal data and shall include a body corporate, partnership, society, trust, association of persons, government company, government department, urban local body, agency or instrumentality of the state;

(x) "Data Processor" in relation to personal data means any person (other than an employee of the data controller), who processes the data on behalf of the data controller;

(xi) "Data Subject" means any living individual, whose personal data is processed by a data controller in India;

(xii) "Direct Marketing" means sending of a commercial communication to any individual.

(xiii) "Disclosure of personal data" means the dissemination, broadcast, communication, distribution, transmission, disclosure or making available in any manner whatsoever, of personal data;

(xiv) "DNA" means cell in the body of an individual, whether collected from a cheek cell, blood cell, skin cell or other tissue, which allows for identification of such individual when compared with other individual;

(xv) "Government" or "the Government" shall include the Central Government, any State Government and local authority;

(xvi) "individual" means a citizen of India;

(xvii) "interception of a communication" means if a person in the course of its transmission by means of a telecommunication system:

(a) so modifies or interferes with the system, or its operation;
(b) so monitors transmission made by means of the system, or
(c) so monitors transmission made by wireless telegraph;

as to make some or all of the contents of the communication available, while being transmitted to a person other than the sender or intended recipient of the communication.

(xviii) "local authority" shall mean a municipal committee, district board, body of port commissioners ,council, board or other authority legally entitled to, or entrusted by the Government with, the control or management of a municipal or local fund;

(xix) "Maintain" includes maintain, collect, use, or disseminate;

(xx) "Member" means the Member of the Authority appointed under sub-section (3) of section 33 and includes the Chairperson;

(xxi) "Person" means any natural or legal person;

(xxii) "Personal Data" means any data which relates to a living, natural person if that person can, either directly or indirectly in conjunction with other data that the data controller has or is likely to have, be identified from that data and includes any expression of opinion about that person;

(xxiii) "Prescribed" means prescribed by rules made under this Act;

(xxiv) "Processing" means any operation or set of operations whether carried out through automatic means or not that relates to:
(a) The organization, collation, storage, updating, modification, alteration or use of personal data;
(b) The merging, linking, blocking, degradation, erasure or destruction of personal data.

(xxv) "Regulations" means regulations made under this Act;

(xxvi) "Re-identify" means, in relation to personal data that has been anonymised, the recovery of sufficient data from that anonymised data as to be capable of identifying any natural person;

(xxvii) "Sensitive personal data" of an individual means personal data relating to:

(a) Unique Identifier such as Aadhaar number or PAN number;
(b) Physical and mental health including medical history;
(c) Biometric or genetic information;
(d) Criminal convictions;
(e) Banking credit and financial data;
(f) Narco analysis and/or polygraph test data.

(xxviii) "Service Provider" means any person who provides any communication service and includes providers of basic as well as cellular telephone services, internet services and postal services;

(xxix) "Surveillance" means obtaining personal data about an individual and his private affairs and includes:

(a) Directed surveillance which is covert surveillance undertaken for the purposes of specific investigation or specific operation in such a manner as is likely to result in the obtaining of private information about a person whether or not that person was specifically identified in relation to the operation;
(b) Inclusive surveillance which is covert surveillance carried out by an individual or a surveillance device in relation to anything taking place on a residential premises or in any private vehicle. It also covers use of any device outside the premises or a vehicle wherein it can give information of the same quality and detail and as if the device were in the premises or vehicle;
(c) Covert human intelligence service 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 obtained provide access to any personal information about that individual;
(d) Surveillance undertaken through installation and use of Closed-Circuit Television (CCTV) and other systems which capture images to identify or monitor individuals.

Chapter II : Right to Privacy

3. **Right to Privacy**

All citizens shall have a right to privacy which shall not be infringed except in accordance with law and subject to the provisions of this Act.

4. **Privacy when it can be infringed**

Notwithstanding anything contained in any law for the time being in force, the privacy of an individual shall not be infringed, except for achieving any of the following objectives:

(i) Sovereignty, integrity and security of India; strategic, scientific or economic interest of the state; **or**
(ii) Preventing incitement to the commission of any offence **or**
(iii) Prevention of public disorder or the detection of crime; **or**
(iv) Protection of rights and freedoms of others **or**
(v) In the interest of friendly relations with foreign states **or**
(vi) Any other purpose specifically mentioned in the Act.

Provided that any such infringement shall not be disproportionate to the objectives that it aims to achieve;

Provided further that such infringement shall not be made except as per procedure prescribed under this Act or any other Act for the time being in force.

5. **Infringement of Privacy**

For the purpose of Section 3 any of the following, unless authorized by the Act, shall constitute infringement of privacy:

(i) Collection, processing, storage and disclosure of personal data.
(ii) Interception or monitoring of communications sent from or to the individual.
(iii) Surveillance of the individual.
(iv) Sending unsolicited commercial communications to the individual.

6. **What does not constitute infringement of Privacy**

Notwithstanding the above, following shall not be considered to be an infringement of privacy:

i. Publication, by any mode, for journalistic purposes unless it is proven that information so published is such in respect of which there should have been a reasonable expectation of privacy.

Explanation: The reasonable expectation of privacy will be determined on the basis of any one or more of the following: (i) whether the individual is normally in public eye, (ii) the nature of activity that was engaged in, (iii) the place where it was happening, (iv) the nature and purpose of intrusion by journalist, (v) the absence of consent, (vi) the effect on the individual of the publication and (vii) the circumstances in which and the purpose for which the information came into the hands of the journalist.

ii. Processing of personal data for purely personal or household use.
iii. Installation of surveillance equipment for the security of any private premises.
iv. Disclosure of information as per provisions of the Right to Information Act, 2005.
v. Any other activity specifically exempted under this Act.

7. **Act to have overriding effect**

If the provisions of any other Act, or rules or regulations made thereunder, in regard to privacy of an individual, are inconsistent with the provision of this Act, then this Act and rules made hereunder shall prevail;

Provided that if any other legislation provides for safeguards for the protection of personal privacy that are more extensive than those set out in this Act, then the more extensive safeguards shall prevail.

Chapter – III : Collection, Processing, Storage and Disclosure of Personal Data

8. **Applicability of Personal Data Privacy Principles**

(1) No person, that has a place of business in India or that does not have a place of business in India but processes data using equipment located in India shall collect, process, store or disclose personal data except in accordance with the provisions of this Act;

(2) Any person not having a place of business in India but who collects or processes or uses personal data in India, shall nominate, for the purposes of this Act, a representative resident in India.

9. **Collection of Personal Data**

(1) Personal data shall be collected directly from the data subject except if:

(i) the information is part of the public record or has been made public by the data subject; or
(ii) the data subject has consented to the collection of personal data from another source.

(2) When personal data is collected directly from the data subject, the data controller must at any time before the data is processed, take reasonable steps to make the data subject aware of:
(i) the documented purpose for which such personal data is being collected;
(ii) whether providing of personal data by the data subject is voluntary or mandatory under law or in order to avail of any product or service;
(iii) the consequences of the failure to provide the personal data;

(iv) the recipient or category of recipients of the personal data;
(v) the name and address of the data controller and all persons who are or will be processing information on behalf of the data controller;
(vi) if such personal data is intended to be transferred out of the country, details of such transfer.

Provided that when the personal data is collected from other sources under sub-section 9(1)(b) the data controller shall take the steps set out above as soon as reasonably possible after the personal data has been collected.

(3) Personal data shall be collected with the consent of the data subject unless:

(i) such collection is necessary for the compliance by the data controller of any law, decree or ordinance; or
(ii) such collection is mandatory under the provisions of any law for the time being in force; or

(4) Notwithstanding the above, the personal data in relation to any person under the age of 18 shall be collected and processed only with the consent of the natural or legal guardian, as the case may be.

10. Processing of Personal Data

(1) Personal data shall be processed:

(i) in a fair, appropriate and lawful manner; and
(ii) for the documented purpose.

(2) A data controller shall collect and process only such type and amount of personal data as is absolutely necessary to fulfill the documented purpose.

(3) Any data subject may object at any time to the processing of his or her personal data if such processing takes place contrary to the provisions set out in sub-sections 10(1) and 10(2) and the data controller, upon receipt of a notification from the data subject to this regard, shall immediately cease to process the personal information.

(4) The data controller shall ensure that all persons involved in any stage of the processing of personal data shall treat the personal data as confidential and shall only communicate such personal data with persons who are directly employed by the data controller or any sub-contractor of the data controller who is under an obligation of confidentiality.

11. Data Quality

The data controller shall take all reasonable steps to ensure that all personal data processed is complete, accurate and updated where necessary and remains so for the duration that it is under the control of the data controller.

12. **Processing of Sensitive Personal Data**

(1) Notwithstanding anything contained in Section 9 or Section 10, sensitive personal data shall not be collected or processed unless authorized by authority.

Provided that no such authorization shall be required if:

(i) collection or processing of such data is authorized by any other law for the time being in force;

(ii) such data has already been made public as a result of steps taken by the data subject;

(iii) such collection and processing is made in connection with any legal proceedings if such processing is necessary for the purpose of obtaining legal advice or for establishing or defending legal rights;

(iv) data relating to physical or mental health or medical history to an individual is collected and processed by a medical professional, if such processing is necessary for medical care and health of the individual;

(v) data relating to biometrics, physical or mental health, prior criminal convictions is processed by the employer of the data subject for the purpose of and in connection with the employment of the data subject;

(vi) data relating to criminal conviction, biometrics and genetic is processed and collected by law enforcement agencies;

(vii) data regarding credit, banking and financial details of an individual is processed by a specific user under the Credit Information Companies (Regulation) Act, 2005;

(viii) sensitive personal data is processed by schools or other education institutions in connection with the imparting of education to the data subjects;

(ix) the authority has, by a general or specified order permitted the processing of specified sensitive personal data for specific purpose and if possible is limited to the extent of such permission.

(2) The data controller shall ensure that all sensitive personal data remains with him under his direct control at all times and is processed only by the persons employed by it, who are under any compulsion to maintain confidentiality of such data.

13. **Retention of personal data**

(1) Personal data shall only be retained for as long as is necessary to achieve the documented purpose, unless:

(i) it is required by law to be retained for a longer period; or

(ii) the data subject consents to its retention for a longer period; or

(iii) such retention is required by a contract between the data subject and the data controller; or

(iv) it is required to be so retained for historical, statistical or research purposes.

(2) All personal data that need no longer be retained in accordance with sub-section 13 (1) shall either be destroyed or anonymised. During the process of destruction or anonymisation, the data controller shall ensure that unauthorized persons do not gain access to the personal data. The destruction of personal data must be carried out in a manner that ensures that it is impossible to re-identify the personal data once destroyed.

14. **Sharing of personal data**

(1) Personal data processed by a data controller shall not be shared with any other data controller without the consent of the data subject unless:

(i) such sharing is part of the documented purpose; or
(ii) such sharing is for any of the purposes given in Section 4;
(iii) the authority has by order authorized such sharing.

(2) Any personal data so shared shall be processed by all data controllers with whom it is so shared, as per the provisions of this Act.

15. **Security of personal data**

(1) Every data controller shall ensure security of personal data under its control by taking appropriate technological, organizational and physical measures to prevent:

(i) loss or theft of, damage to or unauthorized destruction of personal data;
(ii) unlawful processing of personal data; or
(iii) unauthorized disclosure (either accidental or intentional) of personal data

(2) Authority may prescribe regulations or code of practice laying down standards for technological, organizational and physical measures for protection of personal data and different standards may be prescribed for different classes of organizations.

(3) If a data processor is engaged by data controller for processing of personal data it shall be the responsibility of the data controller to ensure that the contractual arrangement between him and the data processor is such that the data processor processes data only for the purpose for which it was collected, keeps it secure with the same degree of care as the data controller and does not disclose personal data to any third party.

(4) In case of any violation of provisions of Section 15(3) both the data controller and the data processor shall be jointly and severally liable under this Act.

16. **Notification about breach of security**

(1) Where a data controller has reasonable grounds to believe that the personal data of any data subject under its control has been accessed or acquired by any person not authorized to do so, the data controller must, as soon as is reasonably possible after discovering the breach, notify:

(i) the data subject, and
(ii) the Authority

(2) The data controller shall not be obliged to notify the data subject in accordance with sub-section 16 (1) (a) if:

(i) such notification will, in the opinion of the Authority, impede a criminal investigation; or
(ii) the identity of the data subject is incapable of being identified

(3) The notification shall be in writing and shall be:

(i) sent to the last known address of the data subject by registered post with acknowledgement due; or
(ii) published in at least two national newspapers.

(4) The notification shall contain sufficient information as is necessary to enable the data subject to take steps to mitigate the potential consequences of the data security breach, including, if possible, the identity of the person who may have accessed or acquired the personal data and the date on which the data security breach occurred. Provided always that under no circumstances shall the notification include any personal information about the data subject.

(5) The Data Authority may require the data controller to take such other steps as it believes would be necessary and relevant under the circumstances to publicise the data security breach if it believes that such publicity would mitigate the harm caused or likely to be caused to the data subject as a result of the breach.

17. **Access to data subject of data relating to him**

(1) Any data subject shall, after proving his identity, have the right to:

(i) request a data controller to confirm, free of charge, whether or not such data controller has under its control, personal data of the data subject; and

(ii) request a data controller to provide details of the personal data of that data subject under the control of the data controller, including information relating to all third parties who have or have had access to the personal data.

(iii) request the data controller to provide information about the logic involved in automated decision-taking where the personal data of that data subject is processed by automatically for the purpose of evaluating matters relating to him.

(2) Any data controller who receives a request under sub-section 17(1) along with the prescribed fee shall:

(i) Provide the information within 45 days of the date of receipt in a form that is understandable to the data subject; and

(ii) inform the data subject that, in the event the personal data under the control of the data controller is inaccurate or incomplete, the data subject has the right to require the data controller to correct it.

(3) Notwithstanding the above, government may prescribe circumstances under which access to data subject under Section 17(1) may be denied.

Provided that the information may not be given if it is not possible to do so without disclosing information about another data subject who can be identified from that information unless that other data subject has consented to the disclosure of that information.

18. **Updation of personal data by data subject**

(1) A data subject shall, after proving his identity, have the right to request a data controller to correct any personal data relating to him that is under the control of the data controller and that is either inaccurate, incomplete or misleading. A data subject shall have the right to request a data controller to destroy any personal data about that data subject that is either excessive in relation to the documented purpose, is an opinion about the data subject that is based on incorrect facts or has been processed otherwise than in accordance with Section 9 or 10;

(2) Any data controller who receives a request under sub-section 18(1) must either correct or destroy the personal data, as the case may be, unless the data controller can provide the data subject with adequate evidence of the accuracy, completeness and fitness for purpose of the data or the lawfulness of its collection.

(3) If a data subject, disputes the evidence provided by the data controller under sub-section 18 (2) the data controller shall be entitled to refer the dispute to the Data Authority.

19. **Conditions under which these provisions shall not apply**

Nothing contained in Sections 9, 11,13,16,17,18 shall apply to personal data:

(i) processed by persons who are, by virtue of their profession, subject to a code of ethics that prescribes disbarment as a consequence for the disclosure of personal data;
(ii) processed in the interests of national security and/or public order; or
(iii) processed in relation to the prevention or detection of a crime; or
(iv) processed in connection with the apprehension or prosecution of offenders; or
(v) processed in relation to the assessment or collection of any tax or duty or of any imposition of a similar nature; or
(vi) processed in connection with the publication by any person of any journalistic, literary or artistic material; or
(vii) processed in order to carry out historical research or for statistical purposes; or
(viii) processed in order to make disclosures required to obtain legal advice or to conduct legal proceedings or otherwise to establish, exercise or defend one's legal rights; or
(ix) processed pursuant to the orders of a competent court.

20. **Power of authority to exempt**

(1) The authority may, in respect of a given documented purpose and if, in the opinion of the Data Authority, such processing of personal data is necessary, by order, waive the applicability of specific provisions of this Act:

(i) Sovereignty, integrity and security of India; strategic, scientific or economic interest of the state; **or**
(ii) Preventing incitement to the commission of any offence **or**
(iii) Prevention of public disorder or the detection of crime; **or**
(iv) Protection of rights and freedoms of others **or**
(v) In the interest of friendly relations with foreign states **or**
(vi) Any other purpose specifically mentioned in the Act.

(2) Provided that the Data Authority shall satisfy itself in respect of each of the situations set out in sub-sections 20(1)(a) to **Error! Reference source not found.** hat, in the circumstances of the case, the public interest in processing personal data significantly outweighs the loss of privacy that the data subject may suffer as a result of such processing. Every order issued under sub-section

20(1) shall be accompanied by a statement issued by the Data Authority setting out its reasons for authorizing the data processing.

21. **Mandatory processing of data**

(1) Where any data subject is obliged under the applicable provisions of any law for the time being in force, to mandatorily disclose personal data to a data controller, then, notwithstanding anything to the contrary contained in such law or any other law for the time being in force, the data controller shall process such personal data in accordance with the provisions of this Act. Provided that nothing contained in this Act will oblige the data controller to obtain the prior consent of the data subject for such mandatory processing.

(2) Where under the provisions of any law for the time being in force, the personal data of a data subject is required to be published in a public register, the access to such public register must be limited to such persons as are strictly necessary to fulfill the purpose for which the list was intended. All such public registers shall, within 12 months of the coming into effect of this Act, be converted into a digital format under which only anonymised data is available to the general public and personal data of a given data subject is only accessible through a searchable database in response to a specific query.

22. **Trans-border flows of personal data**

(1) No data controller shall transfer any personal data relating to a data subject outside the territory of India unless:

(i) the recipient of the personal data is subject to a law, code of conduct or contract which binds such recipient to adhere to principles of data protection substantially similar to the provisions of this Act including in particular provisions substantially similar to this section relating to the further transfer of personal data from the recipient to recipients in other countries; or

(ii) the data subject consents to such transfer; or

(iii) such transfer is necessary or inevitable in connection with the conclusion or performance of a contract to which the data subject and the data controller are both parties.

(2) 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. Any such transferring data controller shall cause the recipient to take appropriate steps to ensure such compliance and shall remain

primarily responsible for any breach notwithstanding the transfer outside the territory of India.

Chapter – IV : Interception of Communications

23. Interception of Communications

No person, including the Central Government and any State Government and any agency or instrumentality thereof, shall intercept any communication to or from an individual except when such interception is authorized by law, and is undertaken in accordance with the procedure prescribed under this Act or any other Act for the time being in force.

24. Safeguards in case of Interception

(1) Notwithstanding anything contained in any law for the time being in force or in any instrument having effect by virtue of any law –

(i) Interception shall be permitted only for achieving one or more of the objectives set out in Section 4;

(ii) Interception shall only be undertaken with the sanction of the competent authority and only after the competent authority has satisfied itself that the required information could not be reasonably obtained by other means and that the intended interception is proportionate to the objective sought to be achieved.

(iii) Any interception that may result in collateral intrusion (infringement of the privacy of individuals who are not the subject of the intended interception) or where communications relate to religious, medical, journalistic or legally privileged material may be involved, will be subject to additional conditions regarding nature of interception, its duration and sharing of intercepted data, as prescribed.

(iv) Interception shall be for minimum period required for achieving the objective for which it is authorized and the permission to intercept will cease immediately thereafter.

(v) The intercepted communication may not be used as evidence in a court of law. It may however, be disclosed to a person conducting a criminal prosecution to enable him to determine what is required of him by his duty to secure the fairness of the prosecution. The prosecutor may not use intercepted material to which he is given access to mount a cross-examination, or to do anything other than ensure the fairness of the proceedings. The prosecutor may, however, provide access of the material to the trial judge, where there are exceptional circumstances making that disclosure essential in the interests of justice.

(vi) The provisions relating to storage, processing, retention, sharing, security and disclosure of personal data, as laid down in Chapter III,

shall, mutatis mutandis, apply to the storage, processing, retention, sharing, security and disclosure of intercepted communications.

25. **Communication data not to be disclosed**

No telecommunication service provider will use or disclose any communication data relating to an individual except in accordance with the procedure prescribed under this Act or any other law for the time being in force.

Chapter – V : Surveillance

26. **Installation & use of CCTV cameras**

The installation and operation of Closed Circuit TV Cameras (CCTV) in public places shall be in accordance with the prescribed procedure, for a legitimate objective and proportionate and will not be undertaken to identify an individual, or monitor his personal particulars, or reveal in public his personal data, or otherwise adversely affect his right to privacy amounting to a civil wrong.

27. **Protection of CCTV images**

The provisions relating to storage, processing and disclosure of personal data, as laid down in Chapter III, shall, mutatis mutandis, apply to all images that are collected through CCTV surveillance.

28. **Ban on covert surveillance**

(1) No person shall undertake Directed Surveillance, or Intrusive surveillance, or Covert Human Intelligence Surveillance (CHIS) unless it is authorized by the competent authority for a legitimate objective which includes –

(i) National Security or public safety
(ii) Prevention or detection of a crime
(iii) Apprehension of offenders
(iv) Economic well-being of the State
(v) Protection of public health
(vi) Assessment or collection of any tax, duty or other government charge.

(2) Surveillance under sub-section (1) shall be undertaken as per the procedure prescribed under this Act or any other law for the time being in force.

29. **Surveillance information subjected to safeguards**

The provisions relating to storage, processing, retention, sharing, security and disclosure of personal data, as laid down in Chapter II, shall, mutatis mutandis, apply to the storage, processing, retention, sharing, security and disclosure of information collected through surveillance.

Chapter – VI : Direct Marketing

30. **Restriction on Direct Marketing**

No person shall hold or process a personal data base used for direct marketing services, unless –

(i) he is registered with the National Data Registry and one of the purposes of registration is direct marketing;

(ii) he has a record stating the source from which he obtained the personal data; and

(iii) all individuals whose data is contained in the data base have consented to receive direct marketing communication from that person.

31. **Individual may request not to subjected to Direct Marketing**

(1) Any individual may, at any time, in writing, require a data controller to cease, or not to begin, processing of his personal data for direct marketing purposes.

(2) Upon receipt of a notice under Section 30 (1), the data controller shall, once the individual has proved his identity, immediately cease the processing of such personal data.

Chapter – VII : The Data Protection Authority of India

32. **Establishment of Data Protection Authority of India.**

(1) With effect from such date as the Central Government may, by notification appoint, there shall be established, for the purposes of this Act, an authority to be called the Data Protection Authority of India.

(2) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract, and shall, by the said name, sue or be sued.

(3) The Authority shall consist of a chairperson, and not more than two members, to be appointed by the Central Government.

(4) The head office of the Authority shall be at New Delhi.

33. **Qualification for appointment of Chairperson and Members.**

The chairperson and the other members of the Authority shall be appointed by the Central Government from amongst persons who have special knowledge of, and professional experience in, data protection, industry, finance, law, management and consumer affairs.

Provided that a person who is or has been in the service of Government shall not be appointed as a member unless such person has held the post of Secretary or Additional Secretary, or the post of Additional Secretary and Secretary to the

Government of India or any equivalent post in the Central Government or the State Government for a period of three years.

34. **Term of office, conditions of service, etc., of Chairperson and Members.**

(1) The Central Government shall, before appointing any person as the Chairperson or member, satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such member.

(2) The Chairperson and other members shall hold office for such period not exceeding three years as the Central Government may notify in this regard from the date on which they enter upon their offices or until they attain the age of sixty-five years, whichever is earlier.

(3) An employee of the Government on his selection as chairperson or whole-time member shall have to retire from service before joining as the chairperson or whole-time member as the case may be.

(4) The salary and allowances payable to and the other terms and conditions of service of the chairperson and the members shall be such as may be prescribed.

(5) The salary, allowances and other conditions of service of the chairperson or of a member shall not be varied to his disadvantage after appointment.

(6) Notwithstanding anything in sub-section (2), a member may –

(i) relinquish his office by giving in writing to the Central Government, notice of not less than three months; or

(ii) be removed from his office in accordance with the provisions of section 48.

(7) The chairperson or any member ceasing to hold office as such, shall –

(i) be ineligible for further employment under the Central Government or any State Government; or

(ii) not accept any commercial employment, for a period of two years from the date he ceases to hold such office.

(8) A vacancy caused to the office of the chairperson or any other member shall be filled up within a period of three months from the date on which such vacancy occurs.

Explanation – For the purposes of this section, "commercial employment" means employment in any capacity under, or agency of, a person engaged in trading, commercial, industrial or financial business in any field and includes also a director of a company or partner of a firm and it also includes setting up

practice either independently or as partner of a firm or as an adviser or a consultant.

35. **Powers of Chairperson.**

(1) The chairperson shall have powers of general superintendence and direction in the conduct of the affairs of the Authority and he shall, in addition to presiding over the meetings of the Authority, exercise and discharge such powers and functions of the Authority and shall discharge such other powers and functions as may be prescribed.

(2) The Central Government may appoint one of the whole-time members to be a vice-chairperson of the Authority who shall exercise and discharge such powers and functions of the chairperson as may be prescribed or as may be delegated to him by the Authority.

36. **Removal of a Member from office in certain circumstances.**

(1) The Central Government may remove from office any member, who –

(i) has been adjudged an insolvent; or
(ii) has been convicted of an offence which, in the opinion of the Central Government, involves moral turpitude; or
(iii) has become physically or mentally incapable of acting as a member; or
(iv) has acquired such financial or other interest as is likely to affect prejudicially his functions as a member; or
(v) has so abused his position as to render his continuance in office prejudicial to be public interest.

(2) No member shall be removed from his office under clause (d) of clause (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard in the matter.

37. **Meetings**

(1) The Authority shall meet at such times and places, and shall observe such rules of procedure in regard to the transaction of business at its meetings (including quorum at such meetings) as may be specified by regulations.

(2) The chairperson or, if for any reason, he is unable to attend a meeting of the Authority, the vice-chairperson and in his absence, any other member chosen by the members present from amongst themselves at the meeting shall preside at the meeting.

(3) All questions which come up before any meeting of the Authority shall be decided by a majority vote of the members present and voting, and in the

event of an equality of votes, the chairperson or in his absence, the person presiding, shall have a second or casting vote.

(4) The Authority may make regulations for the transaction of business at its meetings.

38. **Vacancies, etc. not to invalidate proceedings of Authority**

No act or proceeding of the Authority shall be invalid merely by reason of –

(i) any vacancy in, or any defect in the constitution of, the Authority; or
(ii) any defect in the appointment of a person acting as a member of the Authority; or
(iii) any irregularity in the procedure of the Authority not affecting the merits of the case.

39. **Officers and other employees of the Authority.**

(1) The Authority may appoint officers and such other employees as it considers necessary for the efficient discharge of its functions under this Act.

(2) The salary and allowances payable to and the other conditions of service of the officers and other employees of the Authority appointed under sub-section (1) shall be such as may be specified by regulations.

40. **Functions of Authority relating to data**

(1) The functions of the Authority shall be –

(i) to monitor and enforce compliance of all the provisions of relating to data by all persons to whom it applies;
(ii) to monitor developments in data processing and computer technology to ensure that such development do not adversely affect protection of data relating to individuals;
(iii) to examine law for the time being in force or policy of the Central Government or the State Governments in order to evaluate the effect they may have on data protection and to give recommendations as to appropriate measures required in order to bring them in line with the requirements of this Act;
(iv) to conduct open house discussions, meetings and consultations among relevant stakeholders, to issue consultation papers based on the outcomes of such discussions and to prepare reports, with or without request, from time to time, on any matter affecting data protection;
(v) when requested to do so by any data controller, to conduct an audit of any or all personal data controlled by that data controller for the purpose of ascertaining whether it is being maintained in accordance with the provisions of this Act;

(vi) to establish, maintain and make available in an online format, the National Data Controller Registry in accordance with the requirements for such registry laid down in Section 43;

(vii) to promote an understanding of the principles of data protection through outreach, education and online programmes;

(viii) to receive representations from members of the public on any matter generally affecting data protection and to gather such information as, in its opinion, shall be necessary for, or to assist it in discharging its duties and carrying out its functions under this Act;

(ix) to suggest to the Central Government or any State Government or any agency or instrumentality thereof on any matter relevant to the operation of this Act;

(x) to receive and investigate complaints about alleged violations of data protection in respect of matters covered under Chapter III and to issue appropriate orders and directions;

(xi) to report to Central Government from time to time on the desirability of the acceptance, of any international instrument relating to data protection;

(xii) to investigate any data security breach and to issue appropriate orders as may be required in order to safeguard the security interests of all affected individuals in the personal data that has or is likely to have been compromised by such breach; and

(xiii) to exercise and perform such other functions, powers and duties as are conferred or imposed on the Authority by or under this Act.

41. **Powers of Authority**

(1) Where the Authority considers it expedient so to do, it may, by order in writing –

(i) call upon any data controller at any time to furnish in writing such information or explanation relating to its affairs as the Data Authority may require; or

(ii) appoint one or more persons to make an inquiry in relation to the affairs of any data controller; and

(iii) direct any of its officers or employees to inspect the records or other documents of any data controller.

(2) Where any inquiry in relation to the affairs of a data controller has been undertaken under sub-section (1) –

(i) every officer, if the data controller is a Government department, urban local body or other agency or instrumentality of the State;

(ii) every director, manager, secretary or other officer, if the data controller is a company; or

(iii) every partner, manager, secretary or other officer, if the data controller is a firm; or

(iv) every other person or body of persons who has had dealings in the course of business with any of the persons mentioned in clauses (b) and (c).

shall be bound to produce before the Data Authority making the inquiry, all such records or other documents in his custody or power relating to, or having a bearing on the subject-matter of such inquiry and also to furnish to the Authority with any such statement or information relating thereto, as the case may be, required of him, within such time as may be specified.

(3) Every data controller shall maintain such records or other documents as may be prescribed.

42. **Power of Authority to issue directions**

The Authority may, for the discharge of its functions under sub-section (1) of section 40, issue such directions from time to time to the data controllers, as it may consider necessary.

43. **National Data Controller Registry**

(1) The Authority shall establish and maintain the National Data Controller Registry for the purposes of this Act.

(2) The National Data Controller Registry shall be established as an online database in order to facilitate the efficient and effective entry of particulars by data controllers.

(3) The Central Government shall prescribe appropriate electronic authentication protocols to be employed by data controllers seeking to register themselves on the National Data Controller Registry.

(4) No data controller shall process personal data of any data subject for a given documented purpose unless such data controller has made an entry in the National Data Controller Registry in the prescribed form.

Explanation – For the removal of doubt, it is clarified that a data controller can process personal data for more than one documented purpose provided that it makes an entry in the National Data Controller Registry for each documented purpose and informs the data subject as to the documented purpose in relation to which his personal data is being processed.

(5) The National Data Controller Registry shall contain the following details of data controllers in respect of each documented purpose for which the personal data is being processed:

(i) Name;

(ii) Address of principal place of business of the data controller;

(iii) Name and address of the nominated representative of the data controller if one has been so nominated under Sub-Section 8(2);

(iv) Description of the documented purpose;

(v) Description of the personal data being processed or to be processed by the data controller;

(vi) Description of the recipients of the personal data or any persons to whom the data controller may disclose the personal data;

(vii) Description of the countries to which the data controller directly or indirectly transfers or intends to transfer the personal data.

(6) The National Data Controller Registry shall be available for inspection by members of the public free of cost through a searchable Internet based interface.

(7) The provisions of sub-section (1) shall not apply to any processing the sole purpose of which is to maintain a public register.

44. **Duty to notify changes**

(1) Every data controller shall be obliged to notify the Authority of any changes in the particulars entered into the National Data Controller Registry in accordance with sub-section (5) of section 43 from time to time.

(2) For the purposes of sub-section (1), the Authority shall establish an Internet based amendment procedure that will facilitate the efficient and effective amendment of the particulars of the National Data Controller Registry.

45. **Application for de-registration as a data controller.**

(1) Any data controller may apply to the Authority for de-registration as a data controller if such data controller has ceased to process personal data on or before the date of the application.

(2) The Authority shall de-register the data controller after it has satisfied itself that –

(i) the data controller has destroyed or anonymised all personal data controlled by it during the period of time that it was processing personal data; and

(ii) the data controller has duly intimated all data subjects whose personal data that data controller was processing that it has ceased to process personal data and that it has destroyed or anonymised all personal data previously controlled by it.

Chapter – VIII : Grants, Funds, Accounts and Audit & Annual Report

46. **Grants by Central Government**

The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority grants of such sums of money as are required to pay salaries and allowances payable to the chairperson and the members and the administrative expenses including the salaries, allowances and pension payable to or in respect of officers and other employees of the Authority.

47. **Fund**

(1) There shall be constituted a Fund to be called the Data Protection Authority of India Fund and there shall be credited thereto –

(i) all grants, fees and chargers received by the Data Authority under this Act; and

(ii) all sums received by the Authority from such other sources as may be decided upon by the Central Government.

(2) The Fund shall be applied for meeting –

(i) the salaries and allowances payable to the chairperson and members and the administrative expenses including the salaries, allowances and pension payable to or in respect of officers and other employees of the Authority; and

(ii) the expenses on objects and for purposes authorised by this Act.

48. **Accounts and Audit.**

(1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such auditor shall be payable by the Authority to the Comptroller and Auditor-General of India.

(3) The Comptroller and Auditor-General of India and any other person appointed by him in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has, in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers and to inspect any of the offices of the Authority.

(4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by him in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and that Government shall cause the same to be laid before each House of Parliament.

49. **Furnishing of returns, etc. to Central Government**

(1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of the telecommunication services, as the Central Government from time to time require.

(2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government.

(3) A copy of the report received under sub-section (2) shall be laid, as soon as may be after it is received, before each House of Parliament.

Chapter – IX : Settlement of Disputes

50. **Appellate Tribunals**

(1) An aggrieved person may, make an application to the Appellate Tribunal for adjudication of any dispute arising between the individual and the data controller.

(2) Any person aggrieved by any order or direction or decision of the Authority may prefer an appeal to Appellate Tribunal, within a period of thirty days from the date on which a copy of such order or direction or decision is received by the aggrieved person, in such form, and verified, in such manner and accompanied by such fee as may be prescribed:

Provided that the Appellate Tribunal may entertain any appeal after the expiry of thirty days if it is satisfied that there was sufficient cause for not filling it within that period.

(3) On receipt of an application under sub-section (1) or an appeal under sub-section (2), the Appellate Tribunal may, after giving the parties to the dispute or the appeal an opportunity of being heard, pass such orders thereon as it thinks fit.

(4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority.

(5) The application made under sub-section (1) or the appeal preferred under sub-section (2) shall be dealt with by it as expeditiously as possible and every endeavour shall be made to dispose of the application or appeal finally within ninety days from the date on which it is received:

Provided that where any such application or appeal could not be disposed of within the said period of ninety days, the Appellate Tribunal shall record its reasons in writing for not disposing of the application or appeal within the said period.

(6) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness of any dispute made in any application under sub-section (1), or of any direction or order or decision of the Authority referred to in the appeal preferred under sub-section (2), on its own motion or otherwise, call for the records relevant to disposing of such applications or appeal and make such orders as it thinks fit.

Chapter – X : Offences & Penalties

51. **Penalty for unauthorised interception of communication**
Whoever undertake interception of any communication made by or to any citizen of India or any communication sent by, or, to, him by any other person in contravention of the provisions of this Act or any other law for the time being in force shall be punishable for such offence with imprisonment for a term which may extend to five years, or with fine which may extend to one lakh rupees, or with both for each such interception.

52. **Penalty for disclosure of intercepted communication**
If any person, who intercepted any communication or has any personal information in respect of any other person in accordance with the provisions of this Act discloses any information or the contents of otherwise than in the execution of his duties under any law for the time being in force or orders of court or for the purposes of the prosecution of an offence under this Act or under the Indian Penal Code, he shall be punishable for such offence with imprisonment for a term which may extend to three years, or with fine which may extend to fifty thousand rupees, or with both.

53. **Penalty for obtaining personal information on false pretenses.**
Any person who knowingly and willfully obtains any record concerning an individual from any person or officer of the Government or any agency thereof under false pretenses shall be punishable with fine which may extend to five lakh rupees.

54. **Penalty for violation of conditions of licence pertaining to maintenance of secrecy and confidentiality by service providers.**
In case of violation of conditions of licence of the service providers, pertaining to maintenance of secrecy and confidentiality of information and unauthorised interception of communication, the service providers shall, without prejudice to any penalty which may be levied under the conditions of licence or any other law for the time being in force, shall be liable for suspension or revocation of their licences.

55. **Penalty for undertaking surveillance in certain cases**
Whoever undertake surveillance in contravention of Chapter V, shall be punishable for such offence with imprisonment for a term which may extend to five years, or with fine which may extend to one lakh rupees, or with both for each such surveillance.

56. **Penalty for disclosure of other personal information**
Any officer or employee of a service provider or the Government, who by virtue of his employment or official position, has possession of, or access to, records of the service provider or the Government which contain individually identifiable information or personal information, the disclosure of which is prohibited under this Act or any other law for the time being in force or which is likely to affect of the right of an individual and who knowing that disclosure of the specific material is so prohibited, willfully discloses such information in any manner to any person not entitled to receive it, shall be punishable with fine which may extend to five lakh rupees.

57. **Compensation**
Any person who suffers damage by reason of any contravention by a data controller of any of its obligations under this Act shall be entitled to compensation from the data controller to the full extent of the damage suffered by that person.

58. **Penalties for Contravention of Directions of the Data Authority**
If a person violates directions of the Data Authority, such person shall be punishable with fine which may extend to one lakh rupees and in case of second or subsequent offence with fine which may extend to two lakh rupees and in the case of a continuing offence with additional fine which may extend to two lakh rupees for every day during which the default continues.

59. **Penalties for Data Theft**
If any person intentionally and without authorization from the data subject or the data controller, acquires or gains access to any personal data, then such person shall be punishable with a fine which may extend to seven lakh rupees and in case of a second or subsequent offence with a fine which may extend to ten lakh rupees.

60. **Penalties for not registering with Data Registry**

If any person processes personal data without first making an entry in the National Data Controller Registry as set out in Section 43, such person shall be punishable with a fine which may extend to five lakh rupees.

61. **Penalties for unauthorised collection, processing & disclosure of Personal Data**

If any person contravenes any of the provisions of Chapter III, such person shall be punishable with a fine which may extend to one lakh rupees and in case of a second or subsequent offence with a fine which may extend to five lakh rupees for each subsequent offence.

62. **Offences by Government Departments**

(1) Where an offence under this Act has been committed by any Department of government, the Head of the Department shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly unless he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section 0, where an offence under this Act has been committed by a Department of Government 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 officer, other than the Head of the Department, such officer shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

63. **Cognizance of Offences.**

(1) No court shall take cognizance of any offence punishable under this Act or the rules or regulations made thereunder, save on a complaint made by the Authority.

(2) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate of first class shall try any offence punishable under this Act.

64. **Offences by companies.**

(1) Where an offence under this Act has been committed by a company, every person who at the time 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 provided in this Act, 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 an 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 also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

65. **Civil remedies**

(1) Whenever any person –

(i) contravenes the provisions of this Act which adversely affect the right of privacy of an individual, or

(ii) fails to maintain or correct on the request of the concerned individual, any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(iii) in such a way as to have an adverse effect on the right of privacy of an individual, the individual may, without prejudice to any other action including initiating criminal proceedings or damages for defamation, bring a civil action against such person for compensation and litigation costs reasonably incurred by the individual.

(2) In any suit brought under the provisions of sub-section (1), the court may order the person to issue a public notice for having wrongly disclosed the personal information of a person which adversely affected the amend the individual's record in accordance with his request or in such other way as the court may direct and pay compensation and litigation costs reasonably incurred by the individual.

Chapter – XI : Miscellaneous

66. **Rights of legal guardians of any individual**

The parent of any minor, or the legal guardian of any individual, who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act behalf of such individual to enforce his right to privacy in accordance with the provisions of this Act.

67. **Civil Courts not to have Jurisdiction**

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter with the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

68. **Other rights and freedoms not affected**

An existing right to privacy of a nature shall not be held to be abrogated or restricted by reason only that such right to privacy is not included in this Act or is included only in part.

69. **Power of Central Government to make rules**

The Central Government may, by notification, make rules for the purposes of carrying out the provisions of this Act.

70. **Power of to make regulations**

The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder for the purposes of carrying out the provisions of this Act.

71. **Rules and regulations made under the Act and notification under section 92 to be laid before Parliament**

Every rule made by the Central Government, and every regulation made by the authority under this Act and every notification issued under section 92 shall be laid, as soon as may be, after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or notification or both Houses agree that the rule or regulation or notification should not be made, the rule or regulation or notification 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 or regulation or notification.

72. **Amendment of Act 21 of 2000**

In section 57 of the Information Technology Act, 2000, in sub-section (1), after the words "under this Act", the words "or any other law for the time being in force" shall be inserted.

73. **Power to remove difficulties**

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, after consultation with the Chief Justice of India, by an order published in the Official Gazette, make such provisions, not inconsistent

with the provisions of this Act, as appear to it to be necessary or expedient for removing the difficulty:

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

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

* * *