Proposed Privacy Bill -2011
(Oct 2011 version)

A Brief Note by Naavi

Presented at Privacy Seminar in Mumbai on 21st January 2011

organized by Privacy India & Others

Background:

India already has a constitutional provision that is believed to provide "Right to Privacy" subject to "Reasonable Restrictions". Courts have already given some guidelines on how this can be interpreted in practice. What is being attempted now through separate legislations is to provide a certain operational clarity to the "Constitutional Right to Privacy".

There has been an attempt to pass a legislation for Privacy Protection in India for quite some time. First serious attempt was made when the Personal data protection bill 2006 was presented to the Parliament in December 2006 along with Information Technology Amendment Bill 2006.

The Personal Data Protection Bill 2006 was a simple 14 section bill. It said that "Personal Data" as defined shall not be collected without "Consent", shall not be disclosed for the purposes of "Direct marketing" or "Commercial Gain". Power to further legislate was left to the Central and State Governments with the proviso that there could be upto three Data Controllers for each State. Exemptions were given for detection of crime, prosecution of offenders or for collection of tax. Reporting to the Data Controller and mandating security and minimum collection principles were also indicated. Three year imprisonment and Rs 10 lakh fine was prescribed for violation along with compensation payable to the victim. Vicarious liability of corporate personnel was also included. Summary trial under CrPC was recommended for grievance Redressal.

However the Bill was not passed and lapsed when the tenure of the previous Parliament ended. The Information Technology Amendment Bill was however passed and became law as Information Technology Amendment Act 2008. (ITA 2008).

ITA 2008 incorporated provisions regarding Privacy protection by prescribing both Civil and Criminal liabilities for protecting Privacy. The rules under the relevant section 43A was notified on April 11, 2011 where the term "Sensitive Personal Information" was defined and body corporates processing such information were subjected to responsibilities such as obtaining consent, collecting for a specified purpose, minimum necessary information, holding it only for the specified period etc. A guidance on "Reasonable Security Practices" for protecting such data was also provided in the notification. Failure to maintain such security would invoke a right to the person who suffers wrongful loss to claim damages.

Additionally, under Section 72A, breach of the terms of a lawful contract for processing personal data was made punishable with three year imprisonment and fine.

The rights that a new Privacy Bill needs to address are broader than what ITA 2008 tries to address. Privacy protection under ITA 2008 is completely dependent on the contractual agreement between the data subject and the data processor. Since the individuals in such cases often are victims of one sided contractual obligations, the protection of privacy rights under ITA 2008 may not be strong in practical terms. A separate Privacy Bill provides statutory protection which cannot be easily overruled by the individual contract between the data subject and the data controller.

Government of India has been in the process of drafting a new version of the Privacy Protection legislation in the form of Privacy Bill 2011. It appears that the draft of the Bill is still undergoing several changes. The following comments are based on one of the latest versions available since October 2011

The first draft of the Bill which was available until a few months back was a massive 94 section legislation which has now been pruned to 73 in the latest version. The different versions indicate the amount of confusion that prevails in the legislating bodies. The latest information indicates that even this draft is prone to further amendments and hence we need to keep our fingers crossed to know the final shape the Privacy law may take.

This fluid state of affairs makes it all the more essential that a reasoned feedback is made available to the Government through seminars such as these so that the legislation may be effective and useful.

Essential Features of a Good Privacy Legislation:

In the light of the above the essential features of a Good Privacy legislation can be identified as follows.

- Providing an enforceable Right to the Citizen
- Establishing an effective monitoring mechanism
- Imposing responsibilities on the data processor
- Defining a noncompliance deterrence structure
- Providing a Grievance Redressal mechanism
- Avoid/Minimize overlapping of provisions with other legislations

Let's analyse some of the key provisions of the Privacy Bill 2011 (PB 2011) under the above considerations.

Providing an Enforceable Right to the Citizen

The most important aspect that we look for in the legislation is what is the Right that is protected and whether it is defined properly.

The PB 2011 states under Section 3 that

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

This states that there shall be a right to privacy but privacy itself is defined only through the definition of what constitutes "Infringements". The Privacy right is created by this law by defining the circumstances under which the right to privacy can be infringed. For all practical purposes, in future, this law will prevail over everything else including the interpretations of the Constitution when there was no such law.

The first observation on the Bill is therefore a thought that It would have been more effective if the "Right to Privacy" could have been derived and extended from the Constitution and the Privacy Bill focused only to set up an infrastructure to implement the constitutional guaranteed right and provide such clarifications as are necessary for the implementation.

By attempting to define the Right to Privacy by law we may be imposing restrictions on an extended interpretation of the "Right to Privacy". What the current approach has done is to define the "Right to Privacy" by the set of exclusions mentioned in the Bill which relate to how the data related to the person should or should not be handled. "Privacy Protection" under the Bill therefore does not go much beyond "Data Protection".

A thought has to be given to whether it is feasible to define "Right to Privacy" beyond "Data protection". But this is an intellectual discussion beyond the scope of this note.

Under Section 5, four specific types of infringements are defined. Accordingly, the following activities shall be construed as infringements if they are undertaken in a manner not specifically authorized in the Act.

1. Collection, processing, storage and disclosure of **Personal Data**
2. Interception or monitoring of **communications** sent from or to the individual
3. **Surveillance** of the individual
4. Sending **unsolicited commercial communications** to the individual

Section 4 and 6 indicate "When the Privacy Right can be infringed".

Under Section 4, it does not constitute infringement if privacy Rights are breached under the following circumstances.

1. sovereignty, integrity and security of India, strategic, scientific or economic interest of the State
2. Preventing incitement to the commission of any offence
3. Prevention of public disorder or detection of crime
4. **Protection of rights and freedoms of others**
5. In the interest of friendly relations with foreign states

Under these exemptions the provision on "Protection of rights and freedoms of others" is vague. It is perhaps meant the "Right to Freedom of Expression" and "Right to Information". It is better if the intention is clarified as otherwise such vague provisions are liable to be misused. Even "Preventing incitement" is too vague and is most likely to be misused. "Prevention of public order" can be extended to all cases of politically motivated issues and is another source of misuse. "Security of India" used in the first sub clause would have covered the cases of offence or crime and hence points 2 and 3 above can be deleted while point 4 could be made more specific.

Under Section 6, Publication by any mode for journalistic purpose is also exempt from Privacy unless it is proven that such publishing is of material which is reasonably expected to be held private. This perhaps can be identified with "Freedom of Press".

The rights specified above apply to "Personal Information" which is a very broad set of information about any living individual that is capable of individually identifying the person. The definition of "Personal Information" also includes "Any expression of opinion about that person". [Sec 2(xxii)]

As against this, there is also a definition of "Sensitive Personal Information" under Section 12 which means the following

- UID or PAN
- Physical and mental health including medical history
- Biometric or genetic information
- Criminal convictions
- Banking credit and financial data
- Narco Analysis and/or Polygraph test data

Sec 12(1) indicates circumstances in which Sensitive Personal Information can be disclosed without authorization without being considered as an infringement.

The Act in its entirety applies to "Personal Information". The only special provision that is applicable to "Sensitive Personal Information" is that processing of such information has to be managed by a Data Controller with **a prior authorization** and **cannot be sub contracted** to a "Data Processor".

The inclusion of PAN number as sensitive personal information makes every business entity which draws an invoice or pays TDS for suppliers would become a "Data Controller" under the Act subject to registration and other formalities. It is not clear if it was the intention of the legislation to make every business entity including professionals like Chartered Accountants using the PAN numbers of others as "Data Controllers".

Redefining the basic Principles

If the "Privacy Right" has to be taken beyond "Data Protection", it is necessary to define "Privacy" as a "Sense of personal liberty felt by an individual without the constraints felt by him as radiated by people around him".

The availability and disclosure of data about an individual to the people around is the prime reason for these constraints to be felt by the individual. Hence one of the concepts of Privacy is to give the right to the individual to control how much of the information about himself he would try to share with others. Under such a definition, data disclosure becomes a means of eroding the sense of privacy and therefore becomes part of the privacy protection mechanism.

This should then be addressed under three classifications namely, "Personal Data, "Sensitive Personal Data" and "Essential Data".

Essential data is one which the society has the right to know. It includes data on communicable diseases carried by the person etc which has a direct impact on the society. Sensitive personal data is the data which the individual has absolute right to keep confidential like the one which a person would like to keep in his private diary. Personal data is the residual data about the person which includes his basic identity.

The entire gamut of "Consent", "Collection Principles", "Data Security", "Data Retention" etc. should be defined under two levels. Level-I Protection norms should apply to all "Personal Data" and Level-II Protection norms (Stricter than Level-I) should apply to "Sensitive Personal Data".

Essential data by definition is mandatory to be made public and hence can be outside the privacy related controls. It is within the reach of "Right to Information" and "Right to Freedom of Expression". Under certain circumstances some of the "Permitted Infringements" fall into the category of "Essential Data".

The above three way classification of data about an individual and developing principles of collection and disclosure for each classification separately is expected to provide a better foundation for regulation than the present approach where principles of collection, disclosure

etc are common for both "Personal data" and "Sensitive Personal data" and only the security aspects during processing differ between the two.

Establishing an effective Monitoring Mechanism

The Bill appears to suggests a single office of the Data Protection Authority with all the administrative responsibilities.

For settlement of disputes, the Cyber Appellate Tribunal (CAT) constituted under ITA 2008 is entrusted with the responsibility of being the first trial court as regards complaints between a data subject and the data controller.

At present, there is one office of CAT in Delhi which is hardly capable of meeting the requirements of ITA 2008. There is therefore an urgent need to recognize that we need a number of Cyber Appellate tribunals or their Benches to be established in many State capitals so that victims may approach them without prohibitive cost.

Further, it would be better if the role of CAT is retained as a First Appeal Court rather than the trial court.

For this purpose, Data Protection Authority should double up as the Adjudicator for disputes. This may require multiple offices of the Authority to be created in States. Alternatively, the administrative and judicial functions of the Data Protection Authority can be segregated and the Authority can set up the required number of Administrators and Data Dispute Adjudicators operating from State locations.

It may be noted however that Under Sec 40(x) while defining the functions of the Data Authority, it is stated that one of the functions is to receive and investigate complaints about alleged violations of data protection and to issue appropriate orders. This indicates that the Authority is vested with a sort of" Investigatory" and "Adjudicatory" powers but this is not taken into account properly while defining the role of CAT. The conflict needs to be resolved and the roles of the Authority and CAT in respect of disputes need to be properly clarified.

Monitoring of Data Processors

Under the proposed Bill, entry in the National Data Controller Registry is made only by the Data Controllers. Data Processors are not registered with the Data Authority except as a part of the Data Controller's entry.

Hence Data Processors need to be controlled through the Data Controllers through appropriate contractual agreements.

Data Controllers may be imposed an obligation to confirm to the Authority that they have periodically audited the facilities of the data processor and are satisfied with the data security practices maintained by them.

Data Processor Agreement should also provide for reporting of suspected data breach incidents to the Data Controller.

Section 15(3) should be reworded to add that the contractual terms include that "While handling the data entrusted to him for processing, the Data Processor shall exercise all due diligence to ensure that there is no contravention of any of the provisions of the Bill and shall keep the Data Controller immediately informed of any suspected breach . "

Defining Offences

The current structure of offences is too elaborate and needs to be simplified. Several sections are in direct conflict with ITA 2008 and perhaps with Indian Telegraph Act. Hence the chapter X requires substantial reworking.

Offences need to be divided into administrative failures and data misuse. Administrative failures may be covered by civil liabilities while data misuse can be made a criminal offence.

Offences by Data Controllers, Data Processors and third parties may also be segregated and penalties defined appropriately.

Penalties can also be defined based on the type of data involved whether it is "Personal Data" or "Sensitive Personal Data" etc.

Overlapping legislations

It is preferable if the overlapping of different legislations is minimized. The Bill envisages legislation on interception, surveillance, unsolicited communication etc. which overlap with ITA 2008 and Indian Telegraph Acts in particular.

It is better for the Government to consolidate the "Interception" related legislation in one Act applicable to all types of data under transit or storage.

If necessary, such consolidation can be made under Privacy bill and the conflicting provisions removed from ITA 2008 and Indian Telegraph Act. Alternatively one single authority to deal with "Interception" can be created under a new Act such as "Data Interception Act" which can address the issue in its entirety. Though this could mean rearrangement of administrative powers of different departments, it would work better in the long run.

Miscellaneous

It is not clear if it is necessary that a "Direct Marketing Agency" has to be registered separately as envisaged under the Bill. They should be considered "Data Controllers" and handled accordingly. Unsolicited communication for marketing then becomes part of the data controller's usage policy based on the consent.

Under Sec 2(viii), "Consent" is defined to include "Implied Consent". This is in conflict with ITA 2008 which requires "Written Consent". Considering implied consent as consent is an

unacceptable dilution of the principle of consent and must be removed. Consent should be in writing including through electronic documents if accompanied by digital signature.

Under Section 63, no Court can take cognizance of an offence except under a complaint made by the Authority.

Under Section 67, it is stated that no civil court will have jurisdiction in respect of any matter which the Appellate Tribunal is empowered to consider.

Under Section 50, "Any aggrieved person" can approach the Appellate Tribunal for any dispute between the individual and the data controller. It is not made clear that such person needs to be a "Data Subject". Hence any dispute related to data can be brought to the Appellate Authority. It is not clear if the CAT is empowered to hear only Civil petitions or is empowered to hear criminal complaints. This needs clarification.

In summary it appears that the Bill requires substantial review .

Na.Vijayashankar
(Naavi)
15th January 2011