© Naavi

Privacy Rights and Data Protection in Cyber Space

By
Naavi

[Prepared for the Seminar on Privacy Rights and Data Protection in Cyber Space by DSFI, KILPAR and KLELC on October 17, 2008]

India is on the threshold of a landmark legislation. For the first time after more than 61 years of independence, a "Privacy Protection Legislation" has been drafted in the form of a Bill and is under consideration of the Parliament in the form of "Personal Data Protection Act 2006". (PDPA 2006).

Normally "Privacy Protection" legislation flows from the desire of a democratic society to guarantee certain minimum level of human rights expected of a civilized society.

In India, though the Constitution provided for "Privacy Protection" under article 21, it was meant only to protect privacy violations by the State. The privacy right guaranteed under the constitution has been subject to an overriding right of the State for National Security and Law Enforcement requirements.

Individuals interested in Privacy Rights have been waiting a long time for legislative protection of their own individual right to privacy. They are looking forward to a legislation where there is a remedy against privacy invasion by individuals and organizations other than the State. They also are looking forward to a legislation which like the UK Data Protection Act or HIPAA of USA will define the scope of protection and also mandate data processors maintaining a suitable security standards for information protection. These issues assume greater importance when the information is handled in electronic form.

The PDPA 2006 however is a result of the persuasion of the IT industry particularly those who are processing data from UK and other European Countries since the data protection in those countries prohibit cross border data transfer to countries without adequate data protection legislation in their respective countries.

Will the legislation which has sprouted from an Industry initiative, meet the requirements of the Privacy Protection expectations emerging from Human Rights perspective?.. is one of the major points of debate in the light of the draft Personal Data Protection Act which is now on the verge of being a law in India.

While "Privacy Protection" and "Data Protection" are two phases of the same coin, there is a third interest which cannot be ignored before the Data Protection Act becomes a law. It is the interest of the Law Enforcement. Unlike the interests of Human Rights Activists and the IT industry which are complimentary, the interests of the Law Enforcement are mostly in conflict with the requirements of the Individual Privacy Right seekers.

This conflict is a matter of concern more with the IT industry rather than individuals. When Police in pursuance of a crime trail end up on a Social Networking site such as Orkut or baazee.com there are commercial interests that try to block the Police from accessing information which may be vital to the solving of a crime. Often the defense put up by the Orkut or Baazee.com are that the information is protected by the "Privacy rights" of some one else or that they are to be treated as "Intermediaries" and should not be harassed.

In some of the recent terrorist cases, Police have encountered employees of respected IT companies such as Wipro or Yahoo.com engaged in terrorist activities while they were in service. The activities of the employees immediately prior to their being found out or dismissed from service become important evidence required by the Police to prosecute the erring employees. There have also been instances of Phishing frauds in Banks where the access records of the fraudster are captured in the IT systems within the Companies. In such cases, investigators would like to pick up evidence from these systems, forensically analyse and also present them to the Courts.

Obviously any request of such nature will be highly disconcerting for the IT company and there will be a strong opposition for any such intrusion into the data networks of Companies by the Police even if it is for a worthy cause.

One of the problems why this conflict cannot be easily resolved is that the trust level between the law enforcement and the public is not very high. Companies may fear that any information shared with the investigator may ultimately leak out to their adversaries and result in damage to their business.

The biggest challenge to "Privacy Protection" legislation will therefore be to resolve or substantially reduce the conflict in "Data Disclosure" between the Companies and the Law enforcement.

In this context law enforcement should also be concerned with what is contained in the Data Protection legislation before the Parliament. The most important aspect they would look forward to is if there are any restrictions or procedural guidance on "Information Interception". For example, Police would be happy if they can have real time access to the ISP's servers to watch the dynamic IP address allocations or if they can access the Mobile service provider's server logs to watch the IMEI numbers of the customers etc.

Thus the proposed legislation is keenly watched by three segments of the society namely the Human Rights Observers, Corporate entities using IT (may be Web portals, E-Commerce companies as well as non IT Companies) and the Police.

If it has taken 60 years to draft a legislation for Privacy Protection, one can easily say that any revision there of is unlikely to happen in near future. It is therefore necessary that the fist legislation itself should be a result of thorough analysis and consultation of all affected parties. At the same time, if experts donot intervene now and place their valuable suggestions with the legislators, they will regret later if the legislation is faulty.

© Naavi

The Issues Before Us:

In the light of a new law being passed in India for Data Protection, the following questions arise

1. What does the "Data Protection Bill 2006" protect? And for Whom? .

2. Is Data Protection Bill meant to protect the privacy of individuals under the Human Rights Charter? Or Is it a means of protecting data in the hands of IT Companies from theft or misuse?

3. Since ITA 2000 already has many provisions that criminalize data vandalism and some more amendments are also due in the ITA Amendment Bill before the Parliament,

4. Are there any conflicts between the proposed new ITA 2000 and the Data Protection Bill?

5. What are the powers given to Police under the Data Protection Bill as well as under the amended ITA 2000 for information interception.

6. What are the protections given to Intermediaries and Companies which curtail the powers of the Police to seek information from them during investigations?

7. If Police are given any exemplary powers to invade privacy under any contingent circumstances, are there enough checks and balances to prevent the misuse of such powers?

8. How does the proposed law compare with similar legislations elsewhere.

9. Does the proposed law impact the area of "Information Security"? "Corporate Governance"?.. etc

We shall therefore examine the provisions of Privacy Protection in India under the Constitution, Proposed Data Protection Bill and the Proposed Amended ITA 2000 with the certain issues that arise in Cyber Space and confront the Law enforcement.

This note tries to capture some points in this regard to enable a debate by experts.

Right to Privacy:

The European Convention on Human Rights (Article 8), The Universal Declaration on Human Rights (Article 12) and the Treaty on Civil and Political Rights (Article 17) are a few of the International conventions which have focused on the need for Privacy Protection as an essential ingredient of a civilized democratic society.

.
In India, the Supreme Court has stated in some of its judgments that Right to Privacy can be inferred from Article 21 in the Constitution as a "Fundamental Right" though not directly indicated.

The article states that "No person shall be deprived of his life or personal liberty except according to procedure established by law". "Personal Liberty" here includes "Privacy". However, like all fundamental rights, this is also restricted by the power of the State to restrict the right in the interest of the Security of the State etc.

The judgments given by the Supreme Court, indicate

1. That the individual's right to privacy exists and any unlawful invasion of privacy would make the 'offender' liable for the consequences in accordance with law
2. That there is constitutional recognition given to the right of privacy, which protects personal privacy against unlawful governmental invasion
3. That the person's "right to be let alone" is not an absolute right and may be lawfully restricted for the prevention of crime, disorder or protection of health or morals or protection of rights and freedom of others

These powers can be invoked against the State through a Writ petition in High Court or a Supreme Court.

Experts however feel that the remedy provided by the Constitution when the Privacy of an individual is breached in the course of a commercial transaction by another non Government entity is still inadequate and cumbersome.

In USA, several legislations such as the Privacy Act, Electronic Communications Privacy Act, HIPAA, GLBA etc address the issue of Privacy. These legislations ensure that there is a "definition" for the information whose Privacy is protected, need for secured storage, need to restrict access on need to know basis, ensure accuracy, ensure transmission security etc. There are Civil remedies and Criminal liabilities for breach of Privacy. At the same time, there are enough exemptions to facilitate information release for Law Enforcement, Judiciary and other contingencies.

Legislations such as HIPAA Contain such detailed security instructions for protection of Privacy that it can substitute an Information security manual.

Status in India

In India we are groping in the dark of what information is Privacy Protected? What are the remedies? What is expected by data processors? Etc. These are essential provisions that need to be made before we can effectively provide legal protection for the Privacy of individuals.

ITA 2000, under Section 72 protects private information that is obtained by agencies by virtue of powers conferred under the Act and enforces a criminal liability with imprisonment for 2 years and fine of RS 2 lakhs. This could be applied to Certifying Authorities who obtain information from subscribers.

Otherwise under Section 66 of ITA 2000, the Act provides 3 years imprisonment and Rs 2 lakh fine for "Diminishing the value of information". (Breach of confidentiality of any information is interpreted as diminution of its value).

Section 43 of ITA 2000 provides for Civil Remedies in case a person can prove that he has suffered a damage because there has been an unauthorized access to any information and the compensation can be as high as RS 1 crore.

What ITA 2000 fails to protect is cases such as "Cyber Stalking" where privacy intrusion through e-mails or SMS messages creates problems for individuals. If such messages can be brought under "Obscenity" then it may be covered either under Section 67 of ITA 2000. If it is indecent or threatening, it may be brought under IPC. These therefore are essentially the protection available. But harassment of a male or harassement without indecency is difficult to be classified as an offence.

Challenges to Law Enforcement:

Of late there have been many crimes in which the Police have been after IP addresses for E-mails or IMEI numbers for Mobiles where the Police end up getting an ISP's proxy server address. There are anonymizer services which make it extremely difficult to locate the originating IP address of the offender. Compounding the problems, most of the international ISPs and service providers such as Google, Hotmail or Yahoo take pride in not disclosing the identities of IP addresses of their clients under the excuse of a duty to protect Privacy of the individual. In all such cases either the Police have to forget getting information or complete tedious formalities to approach the Interpol through CBI and seek the information. By the time information is available it may be too late for catching the offender.

On the Internet, the "Who Is" information is another area where the Privacy protection is creating hurdles for law enforcement and those seeking genuine legal remedies.

Some of the other requirements of the Law enforcement are

a) Availability of IP address resolution through access to the log records of ISPs on an online interface.
b) Availability of Originating IP address in all e-mails
c) Registration of Anonymizers and banning of unregistered Anonymizers.
d) Cyber Cafes to strictly monitor identity verification or alternatively, Cyber Café access to be provided through an Citizen ID Card or alternatively a Cyber Café monitoring system to be established under the direct control of the State Police

e) Every mobile call to be tracked to the IMEI address and banning the presence of Mobile Phones with fake IMEI address
f) Provision of Mobile number-owner data base online for verification by public like landlines
g) Intermediaries to provide profile information on demand from public through an appropriate procedure such as RTI.

If Privacy legislation is to be respected by the Law Enforcement it should be seen as addressing the requirements of the law enforcement.

What is Data Protection Act?

Whenever we think of "Data Protection Act" we are reminded of the UK /EU initiatives. It must be remembered that the UK Data Protection Act is a comprehensive legislation where there is a definition of what is "Sensitive Private Information" which needs to be protected. What is meant by "Protection", What are the consequences of "Breach", What is the administrative framework for data protection, etc.

Data Protection Act of UK/EU as well as HIPAA ensure that data protection obligations reach beyond its shores whenever data is sent out for processing to other countries.

Indian Data Protection Legislation

In the light of the above discussions let us now look at the two new legislations that are pending in the Parliament as Bills and which may get passed soon, namely the Personal Data Protection Bill 2006 and Information Technology Act Amendment Bill 2006.

First let us look at the few amendments proposed to ITA 2000 for ensuring Data Protection requirements as demanded by the International Outsourcing clients of Indian BPOs. The objective of these sections is to meet the requirements of the Data Protection Act of UK that data can be sent out for processing only to such Countries who have adequate legal protection similar to the UK act. (Comments here are based on the version of the Bill which was commented upon by the Standing Committee and ignores any changes that might have been made later)

Accordingly, it has been proposed as follows:

> ***Sec 43 A: Compensation for failure to protect data (Inserted vide ITAA 2006)***
>
> *Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person,*

such body corporate shall be liable to pay damages by way of compensation, not exceeding five crore rupees, to the person so affected.

Explanation: For the purposes of this section

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

(ii)"reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

To give effect to this section, there is a need to define "Sensitive Personal Data or Information" as well as "Reasonable Security Practices and Procedures".

66 A Punishment for sending offensive messages through communication service, etc.*(Introduced vide ITAA 2006)*

Any person who sends, by means of a computer resource or a communication device,-

a) any content that is grossly offensive or has menacing character; or

b) any content which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or illwill, persistently makes use of such computer resource or a communication device,

shall be punishable with imprisonment for a term which may extend to two years and with fine.

Explanation:- For the purposes of this section, the term "communication device" means cell phones, personal digital assistance (PDA) or combination of both or

any other device used to communicate, send or transmit any text, video, audio or image.

This section is supposed to provide Privacy protection against Cyber Stalking but limits its operation to content that is "grossly offensive or has menacing character." Or content which is "known to be false" and meant to create "annoyance" etc

Section 72 A Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2006)

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with a fine which may extend to five lakh rupees, or with both.

This section has to be read along with the Section 79 (New) which is providing certain exemptions to an intermediary from liabilities.

Section 79: <u>Exemption from liability of intermediary in certain cases</u>

(1) Notwithstanding anything contained in any other law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available by him.

(2) The provisions of sub-section (1) shall apply if-

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or

(b) the intermediary does not-

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission

(3) The provisions of sub-section (1) shall not apply if-

(a) the intermediary has conspired or abetted in the commission of the unlawful act (b) upon receiving actual knowledge, or on being notified by the appropriate

Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

(4) Intermediary shall observe such other guidelines as the Central Government may prescribe in this behalf.

Explanation:- For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.

A Clarification may be required to state that Section 79 does not infringe the rights that an individual may exercise under the earlier section 72 A.

Modification Proposed for IPC:

In addition to the amendments proposed directly to the ITA 2000, the ITA Amendment Bill is expected to modify the IPC as well in certain respects. One of the Privacy related modifications expected is the introduction of a new section 502A as anew chapter XXIA which refers to Privacy Protection.

The new section reads as under:

502 A: Of Privacy:

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with simple imprisonment for a term which may extend to two years or with fine not exceeding two lakh rupees or with both.

Explanation:- For the purpose of this section-

(a) "transmit" means to send electronically a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means

(c) "private area" means the naked or undergarment clad genitals, public area, buttocks or female breast

(d) "publishes" means reproduction in the printed or electronic form and making it available for public

> *(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that*
>
> > *(i) he or she could disrobe in privacy, without being concerned that an image or his private area is being captured; or*
> >
> > *(ii)any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.*

The above addition to IPC is being touted as an important provision in Privacy Protection in India. However it only betrays the lack of distinction between "Privacy" and "Obscenity" or "Voyeurism". It appears that protection against "capturing of a photograph of parts of human anatomy" is being considered as "Privacy Protection" by those who thought of this addition to IPC.

More than anything else, this indicates the need for professionals to step in and contribute towards drafting of a better legislation which protects Privacy as Human Rights Activists want as well as what the IT Industry and the Law Enforcement would desire.

Now having gone through the proposed amendments of ITA 2000 let us look at the proposed Data Protection Act in greater detail to examine if this fulfills the expectations of individuals as a Privacy Protection legislation and the expectations of the BPOs as a reflection of the UK/EU data protection legislation.

Personal Data Protection Bill 2006 (PDPB 2006)

(P.S: A copy of the Bill is annexed)

The objectives of the Bill state that it is s Bill

> *" to provide protection of personal data and information of an individual collected for a particular purpose by one organization and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected therewith or incidental thereto"*

It appears from the objective statement that the Act which follows the passage of the Bill will be meant to be India's "Privacy Act". It covers use of "Personal data" by any organization for any purpose and prohibits disclosure without consent.

The Bill contains only 14 sections distributed as follows:

Section 1: Name, Geographic coverage and effective date

Section 2: Definitions

Section 3: Mandatory Consent for Processing and exemptions

Section 4: Prohibition for disclosure for marketing

Section 5: Compensation for Damages suffered

Section 6: Appointment of Data Controllers

Section 7: Obligations of Data Processors

Section 8: Release of Funds

Section 9: Penalty (3 years imprisonment and RS 10 lakh fine)

Section 10: Liability of Company, its Directors/officers and need for Due Diligence

Section 11: Applicability of CrPC

Section 12: Removal of Difficulty

Section 13: Non Exclusion of other Statutes for similar purpose

Section 14: Power to make Rules

The scope of the Personal Data Protection Act 2006 (PDPA-2006) extends to the "Whole of India". We may remember that since ITA 2000 was passed based on the UN resolution, it has been made applicable to the " Whole of India including Jammu and Kashmir". Presently therefore the provisions of ITA 2000 alone and not PDPA 2006 would be applicable to J&K.

Under section 3, the processing of personal data is permitted without the consent of the person for

(a) prevention or detection of crime
(b) prosecution of offenders
(c) assessment or collection of any tax or duty

We may therefore say that the Privacy protection requirement under the act need not hamper the work of the Police.

Consent of the data subject has been made mandatory for use of personal data for processing. The definition of processing as given is,

> *" obtaining, recording or holding the personal data or information of an individual and carrying out any operation on the information including alternation, disclosure, transmission, dissemination and destruction. "*

Prohibition is specifically mentioned for “marketing” under Section 4.

The need for use of data “Only for the purpose for which it is collected” and “Need to maintain accuracy of data” , the use on a “Need to Know basis”, “Destruction after usage” etc., which are accepted principles of Privacy Protection are to be implied from the section and need elaboration in the rules.

The right of a person to demand information about him stored by a data collector and right to demand that inaccuracies are to be corrected needs to be specified. This “Right to Self Information” is an essential aspect of “Privacy Protection” since inaccurate data can be harmful to the person.

The authorities who collect and process data for detection of crime or for prosecution or for tax purpose etc need to be regulated to ensure that inaccurate data would not be a basis for any action from their end. For this purpose such organizations have to classify the data as “Secret” and “Non-Secret”. “Secret” data has to be deposited with an appropriate “National Security Agency” and reviewed at the level of the DGP of a State. They are considered “Intelligence” material for national interest and need not be disclosed even to the data subject except under intervention of a High Court.

The other information which is classified as “Non- Secret” needs to be notified to the data subject and option given to him to lodge his protest if the information is wrong.

These conditions may required to be incorporated in the Bill.

The “Personal data” as defined by section 2I is too generic and needs to be clarified with the parameters for “De-identification” as done under US HIPAA. For example it needs to be clarified if “IP address” or “IMEI number”, “Whois information” “e-mail address” , “Mobile Number”, “Physical Address”, “Credit Card number”, “Personal Financial Credit information”, “PAN Card number”, “CVV number on a Credit Card” etc of self and dependents comes under the “Identifiers” of personal information or not.

Under Section 11, it is stated that all offences under this act “shall be tried summarily” under the procedure prescribed in CrPc. In as much as Section 9 of the PDA2006 prescribes an imprisonment of 3 years and section 260 of CrPc excludes offences with

punishment exceeding 2 years, there appears to be a conflict which needs to be clarified.

Similarly the liability for Companies under Section 10 of the PDPA 2006 and exemption under Section 79 of ITA 2000 (new) may be in conflict and needs to be sorted out.

It is also necessary to make an impact study on e-Governance projects before the act is passed since most of the e-Governance projects of data will fail the Privacy test as per the proposed law and it will immediately render the projects subject of litigation.

Perhaps we need to consider an implementation schedule both for Private and Public sector as "Compliance Deadlines".

Similarly the powers or limitations thereof the "Data Controllers" need to be explained in the Act itself like the UK Data Protection Act. This may have to deal with the "Registration", "de-Registration", "Compliance audit" etc. Without these provisions the Act will add confusion to the market. If these are to be handled through the notification of rules, then it is better to draft the rules and place it for public comment before the Act is passed into a law with inadequate rules.

It may also be necessary to define procedures for the Police or any other agency permitted to intercept communications and collect private information as was provided under the now defunct POTA.

Multiplicity of Laws

One of the pitfalls to be avoided is to provide loopholes in the law that enables offenders to play one statutory provision against the other and escape or defer scrutiny of offences. This is what frustrates Police and create a fertile ground for abuse of power which Human Rights Activists frown upon.

Without a proper freedom for doing what is considered a duty to the nation, it is unfair to chain the Police with restrictions of Privacy. Some more thoughts on this aspect has to be given in PDPA 2006.

In particular there has to be specific provisions regarding "Intermediary Liability". It would not be out of place even if a mention has to be made in the PDPA 2006 that the

liabilities under Section 10 shall apply even to "Intermediaries as defined under ITA 2000".

Technology as Means of Privacy Intrusion

World over, "Encryption" of data is considered to be a means for protecting the privacy or confidentiality of data. However this is a matter of concern for the law enforcement. Hence there is a demand for "Escrowing" of encryption keys or limitation of encryption technology to the levels which the law enforcement is confident of breaking when required. Technologists would consider this highly objectionable.

Police would like to install "Carnivores" and if possible "Key loggers" or "Spywares" to monitor activities of suspects

Copyright protectionists often include technology for Data Rights Management which are as privacy intrusive as any other spyware.

It is necessary for the Privacy Protection legislations to ensure that it does not try to oppose intrusion by Police while supporting privacy intrusions for Data Rights management purpose.

Summary

While the PDPA 2006 is a welcome effort for a short but effective legislation for data protection, some fine tuning of the Bill would be in order. Alternatively these have to be taken into account during the formulation of the rules though it is recommended that some of the changes may be required in the parent Act itself.

Na.Vijayashankar
(Naavi)
www.naavi.org
+919343554943

© Naavi

Annexure

THE PERSONAL DATA PROTECTION BILL, 2006

As introduced in the Rajya Sabha on 8th December 2006

(Bill No: XCI of 2006)

A

BILL

to provide for protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Fifty-seventh Year of the Republic of India as follows

1. Short title, extent and commencement:

(*1*) This Act may be called the Personal Data Protection Act, 2006.
(*2*) It extends to the whole of India.
(*3*) It shall come into force with immediate effect.

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

(*a*) "appropriate Government" means in case of a State, the Government of that State and in other cases, the Central Government
(*b*) "Data Controller" means Data Controller appointed under section 6;
(*c*) "personal data" means information or data which relate to a living individual who can be identified from that information or data whether collected by a ny Government or any private organization or agency;
(*d*) "prescribed" means prescribed by rules made under this Act;
(*e*) "processing" means obtaining, recording or holding the personal data or information of an individual and carrying out any operation on the information including alternation, disclosure, transmission, dissemination and destruction.

3. Personal data not to be disclosed.

The personal data of any person collected for a particular purpose or obtained in connection with any transaction, whether by appropriate Government or by any pri vate organization, shall not be put to processing without the consent of the person concerned:

Provided that personal data of any person may be processed for any of the following purposes:—

(*a*) the prevention or detection of crime;
(*b*) the prosecution of offenders; and
(*c*) the assessment or collection of any tax or duty.

Provided further that no consent of the individual shall be required if the personal data details of the individual are obtained through sources which have been made public.

4. Personal Data Not to be Disclosed:

The personal data of any person collected by an organization whether government or private, shall not be disclosed to any other organization for the purposes of direct marketing or for any commercial gain:

Provided that personal data of any person may be disclosed to charity and voluntary organizations after obtaining prior consent of the person.

5. Compensation for damages in case of disclosure of data information:

Every person whose personal data or details have been processed or disclosed for direct marketing or for any commercial gain without consent shall be entitled to compensation for damages in such manner as may be prescribed.

6. **Appointment of Data Controllers**

(*1*) The appropriate Government shall, by notification in the Official Gazette, appoint as many Data Controllers as may be necessary for over viewing the complaints relating to processing and disclosing of personal data and claim for compensation:

Provided that there shall not be more than three Data Controllers in a State or a Union Territory.

(*2*)The terms and conditions of service of the Data Controller shall be such as may be prescribed.
(*3*) The appropriate Government shall provide such number of officers and staff as may be necessary efficient functioning of the Data Controller.
(*4*)The procedure for appointment of the Data Controllers, their powers and functions shall be such as may be prescribed.

7. Obligation on organization collecting personal loan:

Every organization, whether Government or private, engaged in the commercial transaction and collection of personal data of persons shall:—

(*i*) report to the Data Controller the type of personal data and information being collected by them and the purpose for which it is being or proposed to be used;

(*ii*) take adequate measures to maintain confidentiality and security in the handling of personal data and information; and

(*iii*) collect only such information that is essential for completion of any transaction with the individual.

8. **Appropriate Government to Provide Money:**

The appropriate Government shall, after due appropriation made in this behalf, provide such sums of money as it may think fit for being utilized for the purpose of this Act.

9. Penalty:

Whoever contravenes or attempts contravene or abets the contravention of the provisions of thisAct shall be punishable with imprisonment for a term, which may extend to **three years or with fine, which may extend upto ten lakh rupees** or with both:

Provided that the compensation for damages claimed under section 5 shall be in addition to the fine imposed under this section.

10. Offence by Companies:

Where a person committing a contravention of any of the provisions of this Act or of any rule, made thereunder is a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention 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 punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

***Explanation*:—** For the purpose of this section:—

(*i*) "Company" means anybody corporate and include a firm or other association of individuals; and

(*ii*) "director", in relation to a firm, means a partner in the firm.

© Naavi

11. Summary Trial:

All offences under this Act shall be tried summarily in the manner prescribed for summary trial under the Code of Criminal Procedure, 1973.

12. Power to Remove Difficulties:

If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provision s 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 the period of three years from the date of commencement of this Act.

13. Savings:

The provisions of thisAct shall be in addition to, and not in derogation of, the provisions in any other law, for the time being in force, relating to protection of personal data.

14. Power to Make Rules: The Central Government may, by notification in the Official Gazette make rules for carrying out the purposes of this Act.

STATEMENT OF OBJECTS AND REASONS

In our country, at present, there is no law on protection of personal information and data of an individual collected by various organizations. As a result many a time, personal information of an individual collected for a particular purpose is misused for other purposes also, primarily for direct marketing without the consent of the individual.

The personal data of an individual collected by an organization is at times sold to other organizations for paltry sum in connivance with the employees of the organizations. These organizations with the competition to out do each other enter into the privacy of individual by making direct marketing calls.

There has to be some internal confidentiality standard within the system so that personal information of an individual may not be transf erred to others, which, at times, causes a lot of distress and embarrassment.

In many countries this right of individual has been recognized as basic civil right as an extension of right to privacy and laws have been enacted to protect the personal data of individuals.

Accordingly, there is a need to have a law in our country also for protection of personal information to ensure that personal information of an individual collected for a particular purpose should be used for that particular purpose only and is not revea led to others for commercial or other purposes.

Hence this Bill.

VIJAY J.DARDA

FINANCIAL MEMORANDUM

Clause **6,** of the Bill empowers the appropriate Government to appoint Data Controllers for over viewing the complaints relating to processing and disclosing of personal information and claim for compensation. Clause **8** provides that appropriate Government shall make the funds available for being utilize for the purposes of this Act. Since the expenditure in respect of UTs shall be borne out by Central Government, the Bill if enacted will involve expenditure from the Consolidated Fund of India to the tune of rupees one crore per annum.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 14 of the Bill empowers the Central Government to make rules for the purposes of this Bill. The rules will relate to matter of details only, the delegation of legislative powers is therefore of normal character

© Naavi

Suggestions for Modification of PDPA 2006
By

Naavi

1. The Personal Data Protection Act (PDPA 2006) which is presently before the Parliament in the form of a Bill defines "Personal data". There is also the definition of "Processing". However there is no specific definition of "Data Subject" or a "Data Processor" as entities. These definitions will add to the clarity of the legislation and are required.

2. It is necessary to define the term "Sensitive Personal Data" which should be the personal data to be protected under the Privacy Act.
    a. A reference is already made in the ITA Amendment Bill 2006 about Sensitive Personal Data which is yet to be defined. There should preferably be an unified definition applicable for both acts.
    b. The term "Sensitive Personal Data" is also defined in UK Data Protection Act using certain parameters. HIPAA also distinguishes Data as Identifyable Individual Health Information along with 18 parameters that are called "Identifiers. Sensitive personal data definition under UK Data Protection Act includes racial information, political opinions, religious beliefs, trade union memberships, health information, past crime information etc. HIPAA Identifiers include several parameters including name, address, etc but focuses mainly on Health Information.
    c. However the PDPA-2006 simply talks about "Personal information" without specifying if it is related to health, Political affiliation, Financial etc.
    d. It may also be necessary to clarify if the Act extends to oral and written data as in HIPAA or limited to Electronic Data only as in UK DPA.
    e. This needs to be reviewed and a suitable definition of "Data", "Sensitive personal information" and "De-Identified Information" needs to be added to the Act.

3. "Data Controllers" are defined in such a manner that there will be one or more data controllers in each state.
    a. There is a need to define a single all India controller similar to the "Data Commissioner" of UK. Otherwise procedures followed by different Data Controllers may not synchronize and control and monitoring of breaches will be difficult. An office of Federal Data Controller by whatever name the office is called needs to be created.
    b. There has to be a compulsory registration of data processors and de-registration when required which should ban them from data processing.
    c. Will this introduce the "License Raj" in information processing"? Will it be feasible to register a website or a Company which processes data and de-list them? If it is not done what is the effectiveness of a law? Will it only be a paper tiger? ..are some issues that needs to be thought of.

4. While penalty in the form of imprisonment and fine has been proposed, the civil remedy to a data subject has been guaranteed only when the information is used without consent for commercial gain. There needs to be a proper definition of the rights of the data subject such as when the information is used for say harassment, stalking or defamation etc which are not for "Commercial Gain".

5. The provisions in PDPA-2006 also ignores the established principles of Privacy protection which requires
    a. Information collected for a specified purpose has to be used for the purpose alone.
    b. Information can be used by a data processor within his organization only on a "need to know basis"
    c. Information collected has to be removed out of active use after its purpose is completed.
    d. Information under custody needs to be secured properly etc

    These principles need to be covered.

6. Under the obligation of data processors, mention is made about "Reporting" the type of data and the purpose for which it is being proposed to be collected. But there is no mention that this should be informed to the data subject before getting his consent. The principle of default "Opt Out" when consent is sought needs to be considered.

7. There is a need to prescribe obligations as found in HIPAA such as the need to have a "Privacy Policy", need to designate a "Privacy Compliance official". Instead of leaving everything to the formation of "rules" it would have been better if the Act itself had prescribed certain minimum conditions such as a need for "Privacy Practice Statement" before collection of data from any data subject and binding the data processor to the declarations made therein. This would also have provided a benchmark for the Data Controller to register organizations and de-register them if they violate the essential principles.

8. The penalty of 3 years and Rs 10 lakh fine is grossly insufficient in the context of data protection. Also, there is no distinction for offences committed by accidental disclosure or by negligent security measures or obtained by deceit or fraud. HIPAA prescribes punishment upto 10 years for information obtained by misrepresentation and for commercial gain. There is a need to therefore introduce graded increase in the punishment from less than 3 years for accidental disclosure to at least upto 7 years for privacy breach with knowledge and/or gross negligence and obtaining of private information by fraudulent means.

9. While there is a "Summary Trial" procedure suggested by the Act, there is lack of clarity as to whether the process would be affected by the fact that the punishment term is more than 2 years.

10. In view of the overlapping of PDPA and ITA 2000 and the exemplary protection given to Intermediaries under ITA 2000, there is a need to specifically mention under PDPA that the provisions of this Act in respect of Privacy protection will not be protected under Section 79 of ITA 2000.

11. India is unlikely to remain only as an International Data processor requiring the Data Protection Act just to satisfy our business partners in EU. Sooner or later India may also outsource data processing to other countries. Hence there is need to include provisions such as "Prohibition of Transfer of data out of India" except under appropriate security in the destination country as in Data Protection Act of UK/EU. Such provisions need to also incorporate the need for Business Associate Agreement as in HIPAA.

12. Under "exceptions" only three instances have been mentioned in the Act namely, prevention or detection of Crime, Prosecution of Offenders and assessment or collection of any tax or duty. There is a need to consider expansion of this with provision for right of the public to seek information in some exceptional circumstances such as in the interest of public health, important recruitments such as Police, Judiciary, Information Security officers in private sector etc. Some times health information may have to be divulged to the personal representatives of the data subject and also to the legal heirs. PDPA needs to provide for such exemptions. The Malaysian Data Protection Act contains a good list of exemptions which need to be looked into and adopted in the Indian Act.

13. There is need to provide a comprehensive list of "Exemptions", "Permitted Disclosure" and "Mandatory Disclosure" along with the procedures involved in the invoking of each of these exceptions and the records to be kept regarding the circumstances under which the exceptions were invoked.

14. PDPA needs to also ensure that its provisions take care of and are not in conflict with legislations or practices such as Right to Information Act or Inter Bank exchange of Credit information etc. The least that can be done to preserve public interest along with Privacy rights of individuals is to ensure that in the event any information is sought from an authority under RTI, which is likely to infringe on the Privacy Rights of an individual, such an individual should be informed and given an opportunity to raise an objection. The objection may be intimated to the person requesting the information who may have to indemnify the authority for

any loss or damage claimed on account of the Privacy breach. However the national and public interest considerations should always prevail over the Privacy rights and the individual who raises the objection may have to substantiate his claim under a proper procedure for grievance handling to be set up.

15. The PDPA itself should provide for "DPA Adjudicators" who may award compensation arising out of the provisions of the Act. The Data Controllers can also be considered for the responsibility. However, since Data Controllers need to discharge administrative functions, it is better not to load the judiciary function involved in adjudication also to them. Appropriate procedures as well as provisions for appeal etc need to be provided.

16. It may be a good idea to consider defining certain parameters as "Identifiers". Clarification may be required on when a "Cookie" can be considered an "Identifier", When "IP Address" Can be considered as an identifier etc. It is suggested that if an information can be used along with other available information for the identification of the person, it can be considered as an identifier. Under this definition, an IP address in the hands of an ISP who has the last mile access records may be considered as an "Identifier" in his hands while a website which collects the information as a broad indication of the geographical area from which a person has accessed the website, it is not an identifier.

17. It is also necessary to specifically define the roles of some Internet intermediaries in providing information such as "Who Is" information. Generally information which is essential for identification of a website owner for legal action must be revealed on request from an identified person. The names of owners of an e-mail address, social networking profile, website etc must be made part of the "Right to Privacy Information" which should be part of the PDPA.

Na.Vijayashankar
(Naavi)
+919343554943
www.naavi.org