

In Quest of a Good Privacy Law

A viewpoint..In the light
of the Proposed Privacy
Bill 2011
Naavi

1

Naavi

www.naavi.org

What is a good law?

- It Should
 - Meet a desired purpose
 - Be Simple, Clear, Practical
 - Be amenable for voluntary compliance by a majority
 - Incorporate reasonable deterrence mechanism
 - Avoid duplication and multiple coverage in different statutes
 - Contain Quick, simple and economic process of grievance redressal

2

Naavi

www.naavi.org

ITA 2008 ..

- ITA 2008 already has provisions towards
 - What is sensitive personal information
 - What reasonable security has to be provided by Body Corporates towards such information
 - What are the Civil and Criminal liabilities for breach
- However
 - ITA 2008 Applies only to electronic data
 - Has built in escape clauses for business entities to avoid liabilities (in the definition of reasonable security)
 - Privacy Right Can be easily frustrated by contracts
 - Is therefore inadequate for protecting Privacy of individuals

3

Naavi

www.naavi.org

What this Privacy Bill can do

- Privacy Right is already considered as a guaranteed Constitutional right
 - A Privacy Law can assist citizens by giving the operational mechanism to implement the constitutional guarantee
- However,
 - If we attempt to redefine the Privacy Right through this law, we may actually dilute the presently available right
 - There is therefore need for caution in drafting this kind of law

4

Naavi

www.naavi.org

How is Privacy Right Defined?

In Privacy Bill 2011.

5

Naavi

www.naavi.org

Defining Privacy Right through right to infringe..

- Section 3 states
 - "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"
- The definition throws up the questions..
 - Is it recognizing other laws also which can infringe the Privacy right?
 - Will this definition tend to override the constitutional guarantee in practice?

6

Naavi

www.naavi.org

First Observation..

- There is a need to Review the Definition
 - We need to make a strong reference to “Right to Personal Liberty” as stated in the Constitution and declare that this Act is an
 - “Act to provide operational support to guarantee the Right to Privacy as a part of the fundamental right of a Citizen of India under Article 21 as interpreted by the Supreme Court of India on various occasions”.
 - Should be in the preamble. ..Could also be brought into the definition clause if required

7

Naavi

www.naavi.org

Definition part in this Act...

- May be limited to define
 - the Due Process of Law
 - By which any person who deprives the Privacy of another person can defend himself from liability.
 - The onus to prove due process should be on the person who is depriving the right.
 - There should be no other law that can authorize deprivation of privacy
 - If infringement is permitted in multiple acts, there is no reason why we need to call this Act as “Privacy Act”.
 - The due process of law should ensure that nothing is left to the administrative discretion except under
 - Really emergent circumstances and
 - in true National Interest
 - which should be reviewed immediately and penalized if found to be inadequate

8

Naavi

www.naavi.org

Due Process of Law consists..

- **Authority**
 - Who are the persons/organizations authorized to access
 - Personal information/Sensitive Personal Information
- **Purpose**
 - What are the circumstances under which the authorized persons can exercise the Right of privacy invasion
- **Permitted Process**
 - What is the process to be adopted

9

Naavi

www.naavi.org

Due Process of Law consists..2

- **Documentation**
 - How will the process be documented
- **Review**
 - Who will review and when
- **Punishment**
 - To the designated authority for violating the permitted process
 - To others for infringement

10

Naavi

www.naavi.org

Information Privacy and Personal Privacy

- The Right To “Personal Privacy” is a concept which is beyond “Personal Information Privacy”.
- Personal Privacy is
 - “A State of Mind where a person feels liberated from the constraints of the presence of people around him” or
 - simply “A Right to be left alone”

11

Naavi

www.naavi.org

Information Privacy and Personal Privacy..

- It is my considered opinion that
 - Right to Personal Privacy can be protected only through “Regulated Anonymity” and not by merely regulating “Information” related to a person
 - Provided the Regulators are Trustworthy
- However, Information Privacy Regulation is accepted as an essential part of the regulation and because of this limited perception of Privacy most privacy regulations end up as “Data Protection”
 - Privacy Bill is no exception to this rule

12

Naavi

www.naavi.org

Present Observations

- Though I strongly advocate a relook at the basic concept of Privacy
 - to take it beyond “Information Privacy” to “Personal Privacy”
- Though I consider the Privacy bill as primarily an attempt at Information Privacy Regulation,
- And consequently, I suggest a total redrafting of the Bill,
 - For the purpose of discussions in this seminar, I present a few observations on the draft Bill as presented by the Government...

13

Naavi

www.naavi.org

Key to Information Privacy is

- How we classify Personal Information
 - As Personal Information Per se
 - As Sensitive Personal Information
- I suggest that we need to add a new classification namely Essential Personal Information”
 - which the society should have a right to know.
 - Defining part of personal information as “Essential Information” puts an onus on the individual to deal with the society fairly and keep people around them adequately informed.
 - This involves a “Faithful” “Disclosure”.
 - Eg: Premarital disclosure of AIDS/inability to bear children etc
 - Pre-employment disclosure of criminal convictions etc
 - Website ownership data/content ownership data for invoking due process of law if required by a victim

14

Naavi

www.naavi.org

Essential Information...

- Defining Essential information is another way of stating that
 - if another person accesses such information without consent of the data subject,
 - no infringement would be recognized
 - However, the Right to access “Essential Information” without consent can also be subject to due process of law and different organizations may be given different rights in this respect

15

Naavi

www.naavi.org

Infringement

- The present Bill however uses the traditional concept of defining “Permitted infringements” instead of essential information
- The Bill also introduces a concept of “Proportionate/Disproportionate Infringement”..which needs clarification
 - Sec 4: “ Any such infringement shall not be disproportionate to the objectives that it aims to achieve”
 - Is it intended to be the “Need to know “ concept for the authorities who are permitted to infringe on the privacy?

16

Naavi

www.naavi.org

What is not an infringement (Sec 4)

- Access for the purpose of maintaining
 - sovereignty, integrity and security of India, strategic, scientific or economic interest of the State, friendly relations with foreign states
 - Preventing incitement to the commission of any offence, public disorder or for detection of crime
 - Protection of rights and freedoms of others
 - Is it Right to information? Freedom of Expression?
- Publication by any mode for journalistic purposes
 - unless it is proven that information so published is such that there
 - should have been a reasonable expectation of privacy
 - Is it freedom of press?

17

Naavi

www.naavi.org

Four Dimensions to Privacy evident in the Bill...

- Definition of Infringement under Sec 5 recognizes FOUR Privacy rights by stating
 - Collection, processing, storage and disclosure of **Personal Data /Sensitive Personal data**
 - (Chapter III)
 - Interception or monitoring of **communications** sent from or to the individual
 - (Chapter IV)
 - **Surveillance** of the individual
 - Chapter V
 - Sending **unsolicited commercial communications** to the individual
 - Chapter VI (Direct marketing)

18

Naavi

www.naavi.org

Sensitive personal Information

- **Special Conditions attached to Sensitive Personal Data**
 - Requires prior authorization of Data Protection Authority for collection etc
 - Needs to be reviewed.
 - Cannot be sub contracted by Data Controller
 - Needs to be reviewed
- **What is Sensitive?**
 - 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

19

Naavi

www.naavi.org

Exemption from Prior Authorization

- **Authorized by any other law**
 - Open license for interference from other legislations
 - Can be specific such as Indian Telegraph Act/ITA 2008
- **Already public**
 - Act can prevent misuse of information, though technically it is already in public domain, by stating that “No Data Controller shall use personal data except with prior consent of the data subject”
- **For use in legal defense**
- **For use by an Employer, Educational Institution and under Credit Information Companies (Regulation Act 2005)**

20

Naavi

www.naavi.org

PAN as Sensitive Information

- PAN is used by every business entity which is liable for TDS on suppliers.
 - By virtue of this definition they need to register themselves with the Authority and obtain prior permission in respect of each of his suppliers to receive and process PAN
 - Chartered accountants also need to be considered as Data Controllers
 - Impractical and undesirable
- **UID/Aadhar Number**
 - The need to register and obtain prior authorization from Data Controller will dissuade people from using Aadhar number as identification parameter
- Both PAN and UID should be removed from Sensitive Personal Information

21

Naavi

www.naavi.org

Data Controller and Data processor

- Data Controller means any person who processes personal data
 - one who is entrusted with the responsibility to deal with the data for a specified purpose **by the data subject.**
- Data Processor is any person (Other than an employee of a data controller) who processes the data on behalf of the data controller
 - doesnot have direct relationship with data subject
 - **is bound by a Contract with the Data Controller and his responsibilities are determined by the contractual obligations.**
- Liabilities arising out of a data processing fall on both jointly and severally

22

Naavi

www.naavi.org

What Can be Added...

- Every data controller shall file an annual declaration with the data protection authority that
 - it has satisfied itself that the Data Processor has exercised due diligence sufficient to meet the provisions of the Act

23

Naavi

www.naavi.org

Data Breach Response/Disclosure

- Inform the individual in writing and Inform the authority
- Publish in atleast two national news papers
 - Not required if the information is de-identified information.
- **Data Processor should be required to inform the suspected breach if any to the Data Controller.**
 - Data Breach should be notified on the website of both the Data Controller and the Data Protection Authority.
 - Non reporting of Data Breach should be made a punishable offence.

24

Naavi

www.naavi.org

Security Requirements

- Different requirements should be defined for different types of data
 - Personal Data- Level I
 - Sensitive personal data-Level II
- Disclosure Requirements and Power of different agencies to infringe may also be defined differently for Personal and Sensitive personal data

25

Naavi

www.naavi.org

Grievance Redressal

- Under Sec 67 it is provided..
 - An aggrieved person may make an application to the Cyber Appellate Tribunal (CAT) for adjudication of any dispute arising between the individual and the data controller
 - No need for DCAI permission
- It is Also provided that any person Aggrieved by a decision of the Authority may approach CAT
 - CAT will be both a First trial court and an appeal court
 - Further appeals?
 - We need to mention that further appeals lie with the High Court of the relevant jurisdiction based on the place where the infringement arose or where the data subject resides

26

Naavi

www.naavi.org

Cognizance

- (63) (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.**
 - Likely to restrict the right of a victim to approach CAT under Sec 67
 - Restricts the rights of the citizen. Organizations will develop vested interests. Individuals will be discriminated.. Will breed corruption
- Independent Adjudication wing required
 - an independent Adjudication wing may be created with state wise Adjudicators who may be given quasi judicial powers to adjudicate so that all disputes pass through him.
 - Appeal may go to CAT

27

Naavi

www.naavi.org

Avoid/Minimize overlapping of provisions with other legislations

..

28

Naavi

www.naavi.org

Interception of Communication

- Will conflict with ITA 2008 provisions under Section 69
 - Issue of order
 - Maintenance of records
 - Validity period
 - Destruction
 - Review

29

Naavi

www.naavi.org

A Separate Authority for Interception issues?

- Provisions regarding Interception conflicts with Indian Telegraph Act, Indian Postal Act as well as ITA 2008
 - We may consider a separate legislation as "Communication Interception Act" and remove the related provisions in multiple Acts.
 - Any other measure will breed confusion
- Alternatively all the provisions can be codified under this Act and other provisions should be eliminated.
 - Mere overriding may not be sufficient.

30

Naavi

www.naavi.org

Direct marketing and Unsolicited Messages

- **Direct marketing agent is a Data User**
 - Must be a Data Controller or Data Processor
- If he directly gathers data from the data subject with consent as envisaged in Sec 30, he would be a data controller
- If he gathers the record from any other source he can be considered as a “Data Processor”
 - The purpose of this definition of a Direct Marketing Agent in the Bill is therefore unclear
 - If not properly regulated, it may facilitate Direct Marketing instead of preventing Spam

31

Naavi

www.naavi.org

Consent

- Sec 2(viii) states
 - Consent includes Implied Consent
 - Conflicts with Section 43A where consent has to be in writing
 - A provision which will be easily misused
 - Must be removed

32

Naavi

www.naavi.org

Resident Representative

- Sec 8(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
 - *E commerce sites need to take note*
 - *Is it practical?*

33

Naavi

www.naavi.org

Public Register

- Sec 43(7) says
 - Provisions of 43(1) shall not apply
 - To any processing the sole purpose of which is to maintain a public register
- Sec 43(1) says that
 - “The Authority shall establish and maintain the National Data Controller for the purposes of this Act”.
 - Needs clarification

34

Naavi

www.naavi.org

Summary

- Needs a major review
- Fundamental aspects of definition may be revisited
- Several Changes are required even if Privacy Protection is limited to Information protection

35

Naavi

www.naavi.org

Thank you

Naavi
www.naavi.org

36

Naavi

www.naavi.org