INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Data Privacy in the Indian Scenario

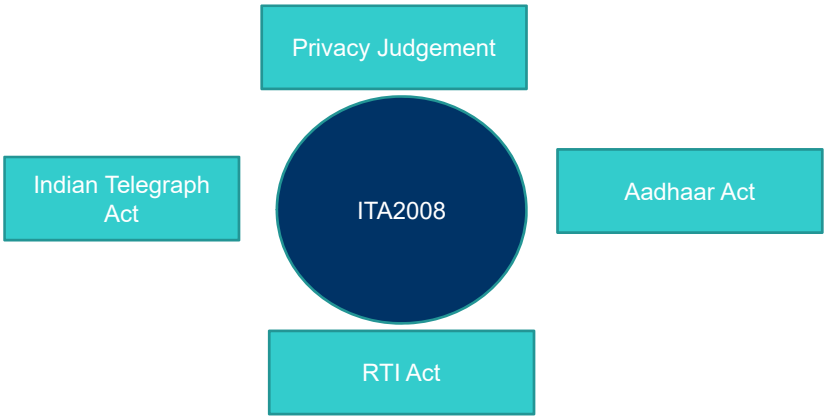
Naavi
July 28, 2018
DISAI, Chennai

1

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Current Privacy Regulatory Scenario

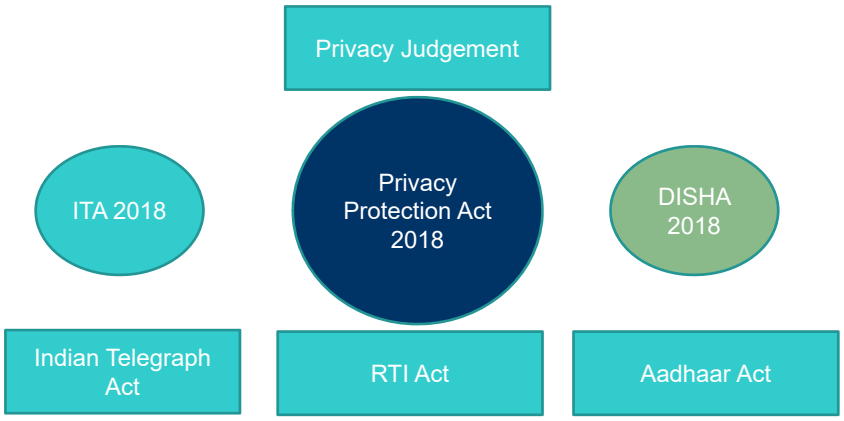


2

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Emerging Privacy Regulatory Scenario



3

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Privacy is a Human Right

- Privacy is a Human Right
  - Desirable in a Democratic Society
  - Held as a Fundamental Right under our constitution
  - But has to also co-exist with other rights which are also fundamental to our constitution and survival
    - Not considered an “Absolute Right” but as a “Right subject to Reasonable Restrictions”

4

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Conflicts

- Right to Freedom of Expression
  - Is also a fundamental right
- Right to Information
  - Is also a respected statutory right
- Cyber Security Right
  - Is a Right for Survival and cannot be relegated into the background
    - Security of State is an exception to Privacy Right

5

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Accepted Reasonable Restrictions

- "Reasonable Restrictions" allowed under Article 19.
  - a) interests of the sovereignty and integrity of India,
  - b) the security of the State,
  - c) friendly relations with foreign States,
  - d) public order,
  - e) decency or morality, or
  - f) in relation to contempt of court,
  - g) defamation or
  - h) incitement to an offence

6

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Scope of ITA 2008 in Privacy Protection

- Defines Personal Information (2011 Rules)
- Defines Sensitive Personal Information (2011 Rules)
- Mandates “Reasonable Security Practice” Section 43A , “Due Diligence” under Section 79
- Provides civil compensation for wrongful loss
- Prescribes 3 years imprisonment under Section 72A

7

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Scope of ITA 2008 in Privacy Protection

- Defines Data Retention Norms under Section 67C and Section 65
- Provides security exceptions under Section 69, 69A, 69B and 70B through due process for exercising powers of interception, powers of decryption, powers to demand information
- Provides a grievance redressal mechanism through Adjudication
  - Additionally, Section 43/66 may also be used for protection of Information Privacy

8

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

The New Introductions

9

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Financial Sector

- Already regulated by RBI and the centuries old Common law principles of Confidentiality of Banking information
- Information Security Guidelines have been provided
  - First under the Information Security Guidelines when Computerization was first introduced in 1980s
  - Internet Banking Guidelines 2001
  - Electronic Banking Security Guidelines under the GGWG committee recommendations
  - Cyber Security Framework in 2016
  - Limited Liability Circular 2017

10

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Health Sector

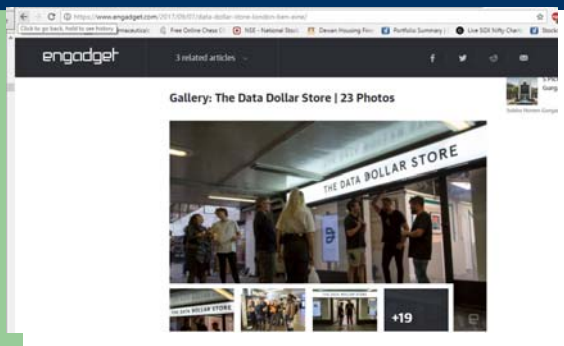
- DISHA 2018
- Digital Health Information created by a service provider is considered as a "Property" of the data subject
  - Similar to the new Californian Privacy Act which recognizes "Selling of personal data by the Data Subject"
    - As a property, data can be sold?..California act recognizes the possibility
  - Have you heard of Data Dollar Store?..in London which barters your data to goods?
- Will introduce a Health Care Sector Privacy Regulator
  - NeHA (National Health Authority of India)
- Will prescribe punishments and civil liabilities for Health data breach (1/3/5 years, Upto Rs 5 lakhs)

11

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Data Dollar Store



https://www.naavi.org/wp/why-we-need-a-data-breach-protection-act-rather-than-data-protection-act/

12

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

EHR Guidelines

- EHR Guidelines preceded DISHA 2018 and is already operative
  - Has provisions on Technical standards for Medical Codes, Transaction Codes , Subject IDs etc
  - Privacy Obligations
  - Security Obligations

13

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

National Health Stack (NHS)

- Sets up a Technical Backbone to support the Ayushman Bharat (Modi Care) program
  - 1.5 lakh Health and Welfare Centers
  - 10 crore Health Insured families and their Health Data storage and Management

14

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Aadhaar

- Aadhaar Act already has special provisions for punishments for any data breach
  - Aadhaar system is a repository of basic demographic data and not associated data such as Health or Financial information or activity data.
  - May be used for KYC
  - Age, Address, Mobile number, E Mail ID, Biometrics are the Privacy related parameters associated with Aadhaar data base which could be subject to Information Privacy compromise
- Efforts have been made to ensure that Aadhaar is used for better Governance without affecting Privacy breach
  - Virtual Aadhaar Scheme

15

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

TRAI Privacy Guidelines

- Definition of Data, Personal Data and Sensitive Personal data as provided in ITA 2000/8 is adequate.
- User owns the data and the Data Controller is only a custodian
- All entities should be restrained from using meta data to identify individual users
- Right to choice, Notice, Express and Informed Consent, to be conferred on the data subjects
- Data Portability and Right to be forgotten to be conferred subject to applicable restrictions
- Framework for sharing of information by TSPs to be developed

16

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

TRAI Privacy Guidelines

- Mandatory to enable removal of pre-installed applications which are not part of the basic functions and enable installation of certified applications at his will
- Grievance Redressal mechanism to be set up for telecom consumers
- Encrypt data in motion and at storage
  - Enable decryption as required under law
  - Encryption norms to be re-visited
- Disclose data breach, share information on threats and vulnerabilities

17

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

TRAI Privacy Guidelines

- Establish a common platform for sharing information relating to data security breach incidences
  - Mandatory for all service providers to be part of the platform
- Sharing of security breach information should be incentivized

18

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Personal Data Protection Act 2018

- Copy of the Bill released yesterday afternoon
  - 112 clauses spread over 15 chapters
  - Section 43A of ITA 2008 removed along with the "Reasonable Security Practice".
  - Follows the general outline of GDPR
  - RTI act slightly modified
    - If personal information release is likely to cause harm which overweighs the public good, it need not be provided under RTI
      - No mention of Aadhaar Act or Telegraph Act

19

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Personal Data Protection Act 2018

- Copy of the Bill released yesterday afternoon
  - 112 clauses spread over 15 chapters
  - Section 43A of ITA 2008 removed along with the "Reasonable Security Practice".
  - Follows the general outline of GDPR
  - RTI act slightly modified
    - If personal information release is likely to cause harm which overweighs the public good, it need not be provided under RTI
      - No mention of Aadhaar Act or Telegraph Act

20

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

When Effective?

- Bill to be enacted
  - Bill to be passed by both houses of Parliament, President to assent and notification to be made
  - Within the next 12 months of enactment a "Notified Date" has to be notified
  - Within 3 months there of, the Authority has to be set up
  - Within 12 months from the notified date, the provisions need to be brought into effect
  - Approximately 18 months may be a reasonable time within which the Act will become operative

21

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Applicability

- Not applicable to processing of Anonymized Data
- Applicable for the processing of personal data
  - by any entity if the processing is in India (collection, disclosure or sharing happens in India)
  - by the State or a Company or any Citizen of India anywhere
  - By any entity wherever located if processing is
    - in connection with any business carried on in India or any systematic activity of offering goods and services to data principals within India or
    - In connection with any activity involving profiling of data principals in India

22

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Section 43A of ITA 2008

- Section 43A of ITA 2008 will be omitted
- Reasonable Security Practice…will no longer be applicable
  - The Rules under 43A will be infructuous
  - Rules under Section 79 may need to be re-issued.

23

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Data Classification

- Sensitive Personal Data
  - Passwords, Financial Data, Health Data, sexual orientation, biometric data, genetic data
  - Official identifier
  - Caste or tribe
  - Sex life, transgender status, inter sex status

24

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Terminology

- Data Principal
- Data Fiduciary
- Significant Data Fiduciary
- Guardian Data Fiduciary
- Data Processor
- Data Protection Authority
- Data Protection Officer
- Adjudicator and Appellate Tribunal

25

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Salient points

- Data Localization
  - One serving copy to be retained in India
- Right to Forget
  - Will be subject to “Adjudication”
- Children Data
  - Age verification and Parental Consent
- Right to Information
  - Subject to determination of harm and public interest

26

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Penalties

- Data Principal can claim damages
- Data Protection Authority can impose fines
  - Rs 5 crore or 2%
  - Rs 15 crore or 4%
  - Rs 1 crore, Per day fine etc
- Criminal prosecution can be launched
  - 3 or 5 years punishment and fines
  - Cognizable and Non Bailable
  - Inspector is the authority
  - Vicarious laibility recognied
  - Extended to Heads of Government departments

27

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Grievance Redressal

- At the DPO level
- At the Data Fiduciary level
- Adjudication as enquiry
- Appellate Tribunal
- Supreme Court
- Civil Court not to have any jurisdiction

28

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Security obligations

- Data Impact Assessment
- Data Audit (annual)
- Data Breach Notification
  - Time to be specified by the DPA
  - DPA will decide if data principals are to be informed
- De-identification and encryption
- Protecting the integrity

29

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

To Sum up

- Personal Data Protection Act 2018 (PDPA 2018) will be the Indian version of GDPR
- Will be operative in about 18 months
  - But should be our guiding principle from now on.
- There will be many challenges ahead of us

30

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Let's Collaborate

- In order
  - to participate in the regulatory exercise and
  - Empower ourselves with knowledge and skills as required and
  - To defend our interests
    - it is necessary for us to collaborate both at individual and organizational level
    - I invite you all to check out www.iadpp.in
      - Indian Academy of Data Protection Professionals
        - As a collaborating platform

31

Naavi

INDIAN ACADEMY OF DATA PROTECTION PROFESSIONALS

Thank You

Naavi
9343554943
naavi@naavi.org
www.naavi.org

32

Naavi