Whitepaper

EU Adequacy Assessment of India

DATA SECURITY COUNCIL OF INDIA
Niryat Bhawan, 3rd Floor
Rao Tula Ram Marg
New Delhi – 110057
India
Phone: +91-11-26155070

7th January 2012

DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative

Adequacy Assessment of India

The EU Data Protection Directive (Directive), through Article 25, sets out the criteria for assessing adequacy of data protection in a third country. It provides that 'adequacy' should be assessed on a case by case basis 'in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations'. The assessment takes into account the nature of data, kind of processing performed on the data, rules of law in general and in specific sectors, content of the applicable law and means for ensuring their effective application.

The methodology covers a range of elements such as: (i) formal legal rules and oversight mechanism, (ii) non-legal rules that have been defined and complied with for privacy, (iii) administrative and corporate culture towards data privacy, (iv) hard and soft instruments that are working for privacy enforcement, (v) informal customs and attitudes and even the professional and industry standards that have been followed for data protection. In doing so, the adequacy assessment evaluates the context of information privacy by looking at social, economic and political concerns as well as the international obligations that a country may be subject to.

It is important to note that the draft EU Data Protection Regulations, 2012 (Regulations), which propose to replace the Directive, also provide that transfer of data outside the European Economic Area (EEA) can take place to only those countries that ensure adequate level of protection. While assessing the 'adequacy' of the level of protection, the Regulations propose to provide consideration to the following factors:

i. The rule of law, relevant data protection legislation in force (both general and sectoral), including laws on (i) public security, (ii) defence, (iii) national security and (iv) criminal procedure.

ii. The professional rules and security measures which are complied with in that country as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred.

iii. The existence and effective functioning of an independent supervising authority responsible for: ensuring compliance with the data protection rules and assisting data subjects in exercising their rights.

iv. The international commitments the third country or international organisation in question has entered into.

This white paper attempts to evaluate the adequacy of India's information privacy regime in light of the 'third country' assessment mandated under Article 25 of the Directive. In May 2010, the EU had commissioned a Report (2010 Report) to analyse the adequacy of protection of personal data provided in India. The report was presented by Graham Greeleaf, Professor, Faculty of Law, University of New South Wales, Sydney, Australia. The 2010 Report has been primarily referred to identify the arguments and observations with respect to the adequacy assessment of India. The paper attempts to provide a response against each assessment criteria as identified in the 2010 Report. This paper draws arguments from the social and cultural context prevalent in India, its constitutional provisions, judicial attitudes to information privacy and the legal provisions - generic and specific - to data protection in India. It brings forward the content, procedural mechanism and enforcement structure that has been put forth by the IT Act and Rules.

The paper argues that recent regulatory changes, unveiled by amendment of IT Act and its Rules, have significantly closed the perceived gap in the regulatory and enforcement mechanisms for privacy protection, and made the country eligible to qualify as providing 'adequate protection' from the EU Directive standpoint.

1. Preliminary

The 2010 Report sets out broad methodological criteria to determine India's data protection adequacy. The study includes an analysis, not just of legislative and case law, but also of the wider political, social and surveillance regime in context of information privacy practices prevalent in India. Based on an overall analysis against the identifiable principles under Article 25, the 2010 Report concludes that India does not at present provide adequate protection to personal data in relation to any sector or to the whole of its private sector or to the whole of its public sector.

While the specific contents of the 2010 Report are discussed in detail in the sections below, it is important to mention that the Report was released in 2010 prior to the enactment of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Privacy Rules). In light of this development, the observations made in the Report concerning the lack of definition of 'personal information' or minimal coverage on data security under the IT Act may have become obsolete.

2. Context of information privacy in India

Any discussion on information privacy laws in India must begin with a discussion on the sociocultural contexts or milieu, which have played a significant role in shaping attitudes about privacy. As compared to the West, individual concerns about privacy in India are recent in origin. This is largely associated with the fact that traditionally India has been a *collectivist* society where there was no concrete individualization of rights until the passage of the Indian Constitution in 1950. Since rights belonged to the realm of community/society, there were no specific concerns about individual privacy. Further, technological advances in India have also been fairly recent in origin compared to the Western nations.

However, social attitudes to privacy have been changing over the years with institutionalization of *individual liberty* through legal developments and greater integration of technology in daily lives. Specifically, the *rights discourse* standard set through multiple judicial pronouncements concerning *personal liberty* and *equal protection before law* have paved the way for a privacy regime that recognises individual autonomy over information concerning herself/himself. If viewed in this light, it will be seen that the progress India has achieved in aligning its information privacy laws to international standards in a short time is truly remarkable.

3. Constitutional Basis for Data Privacy and Tort Law:

The concept of individual privacy is well recognised under the Constitution of India, 1950 (Constitution). In this sense, the concept of privacy largely emanates from the Constitution rather than through a development of law of torts (USA), or by extension of the law of breach of confidence (UK) as may be the case in other jurisdictions.

Article 21, Article 19 and Article 14 collectively assure the citizen the right of life, freedom of speech and expression and equal protection of the law. In several judicial pronouncements, Courts have established, defended, or promoted conceptions concerning individual liberty and autonomy. The 2010 Report made the following observations on the ability of the constitution in the protection of privacy:

(i) Strong pro-rights approach of the Supreme Court could be a very significant and positive background factor;

(ii) The development of rights approach has followed a vertical approach and concerns only state action and therefore the protection is not extended for privacy against the private sector;

(iii) The Supreme Court has not made significant advances in the direction of a comprehensive right of privacy (data protection);

(iv) Indian courts have developed primarily from this constitutional basis, rather than by Indian courts developing a tort of invasion of privacy.

… Page 20 & 22 of the 2010 Report

India's Position:

(i) The Indian constitution and the judiciary have followed a consistent approach in protecting and enforcing individual rights, as evidently demonstrated in the numerous cases cited in the 2010 Report. The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of India by Article 21.

(ii) Data protection has only recently emerged as a major issue and cases under Article 21 have not yet involved data protection issues. However, considering the attitude of the Supreme Court towards rights based issues, there is enough evidence to indicate that the Court may be open to an intervention recognising information privacy and data protection as fundamental rights.

(iii) India's legal and regulatory ecosystems are becoming sensitive to Information privacy issues. With the democratic fabric of the society, legal evolution increasingly sensitive and supporting the cause of personal rights and courts taking a proactive role in protecting human rights, India does provide a requisite characterization that the EU Directive looks at in assessing.

(iv) The amendment of the IT Act, and specifically the promulgation of the Privacy Rules in 2011 have brought the private sector under the fold of a strong data protection regime.

(v) The quasi judicial mechanism of Adjudicating Officer, distributed across the Indian states and union territories, role of civil courts, protection against criminal offenses such as identity theft, and removal of the cap on the liability for unauthorized access and privacy violation, significantly enhance the data protection regime in the country.

(vi) The right of privacy as an actionable tort has been recognised by Indian Courts, and tort action for damages resulting from an unlawful invasion of privacy may lie in case of breach of an individual's information privacy.

4. Breach of Confidence

The adequacy assessment makes a positive determination to the possibility of developing Indian law in expanding the protection for breach of confidence. This dimension of legal development relates to the public disclosure of personal information about which the data subject has a reasonable expectation of privacy - usually applied to the relations such as doctor/ patient and banker/customer relationships. The earlier study maintains its observation in this respect as:

(i) *The likelihood that Indian law is developing along UK lines in expanding breach of confidence could be significant to an assessment of adequacy, if most other elements of adequate protection were provided by statute and this area of law provided a useful supplement.*

(ii) *Breach of confidence law does make a significant positive contribution to the general legal context in which data protection laws operate in India*

… Page 24 of the 2010 Report

India's Position

(i) Indian Courts in the past have recognised the legitimacy of a cause of action based purely upon the duty of good faith applicable to protect confidential personal information and trade secrets. Such actions may or may not arise from contractual obligations and are applicable to a wide array of situations where information privacy could be asserted, such as in doctor-patient relationship or as client-attorney privilege or by a witness who has provided critical information to law enforcement agencies, rights of victims of crime etc.

(ii) Section 72A of the IT Act, inserted by the 2008 Amendment, provides explicit protection against the disclosure of information in breach of confidentiality and privacy in breach of a lawful contract. The language used in Section 72A is wide enough to even cover disclosures that are out of the the lawful contract, provided (a) it is without the consent of the data subject and (b) it is made with the requisite intent.

(iii) unauthorised access to information without consent or in breach of a lawful contract.

(iv) Rule 6 of the Privacy Rules requires the consent of the information provider for disclosure of information to a third party. It also prohibit the body corporate from publication of sensitive personal data or information of individuals by private entities.

5. Contract Act

In Europe, especially in the UK, the legal concept such as 'Rights of Third Parties' may provide data subjects in enforcing legal obligations to the third parties which have been conferred a benefit by a contract. In this regard, the 2010 Report made the following observations:

(i) *Indian law is based on the doctrine of privity of contract and it is unlikely that the data subject can enforce the data protection rights.*

(ii) *Standard Contractual Clauses (SCC) against the data importer, but only where the data exporter has 'factually disappeared'. SCC comes into play under Article 26 once Article 25 is not applicable and therefore, if a country aspires to become 'data security state' it can't rely solely on SCC.*

… Page 36 of the 2010 Report

India's position

(i) the Privacy Rules have now been enacted to provide comprehensive protection to 'providers of information' in respect of sensitive personal data or information belonging to such providers. The Privacy Rules are applicable in their whole when the provider of information has a direct contractual relationship with the data processors. However, certain obligations, such as those relating to maintenance of privacy policy or transfer of information to third parties may be enforced by data subjects that are not a party to the contract between the data processor and controller.

6. Information Technology Act:

The earlier assessment takes note of Section 43-A, identity related offenses, the obligations of the body corporate and the mechanism of adjudicating officers and cyber appellate tribunal while discussing its relevance to the adequacy. It evaluates the surveillance provisions as enacted by section 69 and its ramification to privacy. From the adequacy perspective, the study made the following observations on the amendment to the IT Act:

(i) *The Amendment principally covers the provisions for the cyber security, and enacted in response to the Mumbai attack in 2008;*

(ii) *The Amendment covers **a small part** of what is normally dealt with by information privacy / data protection legislation;*

(iii) *The IT Act does **not deal specifically** with data protection, so **core concepts** such as 'personal data/information', 'processing', 'disclosure', and 'consent' are not defined;*

(iv) *Data in entirely non-automated systems would therefore not be covered by the Act, but data in non-electronic form which had previously been the subject of processing could be;*

(v) *The impact of the IT Act on the public sector is minimal.*

… Page 25 to 27 of the 2010 Report

India's Position

(i) The observation that the Act was enacted in response to the Mumbai attack in 2008 is factually incorrect. The draft of amended Act was first proposed on 2006 and finalized well before the Mumbai attack, after detailed deliberations of the Standing Committee on IT, which extended over a year before December 2008.

(ii) The observations reflect the state prior to the notification of the Privacy Rules. The Privacy Rules address the concerns with respect to the ability of the IT Act in dealing with the information privacy/data protection.

(iii) The Privacy Rules bring the core concept of data protection in the country such as the definition of sensitive personal data or information and personal information, processing of the sensitive personal data or information, and privacy principles concerning collection, disclosure, transfer and reasonable security practices and procedures.

(iv) The Indian constitution and strong pro-rights jurisprudence developed by the courts already contribute to enforcing privacy obligations against the State.

7. Content Principles

The principal methodological criteria for assessing the Indian data protection regime are set out by the Article 29 Data Protection Working Party in its document "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" adopted by the Working Party on July 24, 1998. The core criteria, as recommended by the working party are expressed in three sets (i) content principles (ii) additional principles (ii) Procedural and enforcement mechanisms. The discussions, arguments, observations and India's current position with respect to the content principles are as follows:

7.1. Content Principle, Purpose (use) Limitation:

The 2010 Report, which was conducted prior the notification of the Privacy Rules, observed that

(i) The IT Act 2000 does not impose limitations on the internal use of personal information by the organisation collecting it.

(ii) Indian law does not provide adequate protection in relation to the use of personal information.

… Page 42 of the 2010 Report

India's Position

(i) The Privacy Rules, specifically rules Rule 4 (1)(iii), 5 (1), 5(2) (a), 5 (3), 5 (5) now bring specific content with respect to the privacy principle 'purpose limitation'.

(ii) To elaborate further, the Privacy Rules require collection of information for a lawful purpose connected with a function or activity of the collector of information and require the information collected to be used *only* for the purpose for which it has been collected.

(iii) Further, consistent with Article 13 of the EU Directive, there are exemptions under the IT Act and Privacy Rules for national security, defence, prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.

7.2. Content Principles, Purpose (disclosure) Limitation:

The 2010 Report delves into the section 72A to find its relevance for this principle. It identifies the limiting factors such as: (i) provisions of the section applies only to the information obtained from the service (ii) it's applicable only in case of 'wrongful loss or wrongful gain'. The report maintains its observation as:

(i) 'Wrongfulness of either the loss or the gain may be difficult to prove in cases where personal information has been disclosed

(ii) The principle of 'Consent' is not defined in the IT Act

(iii) The relevance of s72A to the private sector is more difficult to assess

… Page 47 of the 2010 Report

India's Position

(i) The Privacy Rules provide significant improvement over the earlier position. They bring the concept of the 'explicit consent', as defined by rule 5 (1). The rule necessitates entities to take the consent 'regarding purpose of usage' before collection of information. Rule 5 (2) binds the companies not to collect information unless it is necessary for the purpose.

(ii) A separate rule 6 has been defined to take care of 'Disclosure of Information', and necessity of taking prior permission for that. The rules 6 (3) and (4) go further by stipulating that entities and their third parties receiving information shouldn't disclose the information.

7.3. Content Principles, Data quality and proportionality principles – Collection limitations

The 2010 Report, while evaluating the position against the principle, relates its observations to the surveillance related provisions of the IT Act as defined in section 69. It made the following observation;

(i) Rule 9 made under Section 69A ITA 2000 (as amended) purports to provide a general prohibition against monitoring or collection of traffic data or information by any party without an authorisation (or attempts or authorizations thereof) under Section 69B, but the source of the offence is not clear. Even if effective, this Rule would only cover collection of data by surveillance, which is significant but limited compared with other methods of data collection.

(ii) In general, Indian law cannot be considered to provide adequate protection in relation to the collection of personal information

…Page 50 of the 2010 Report

India's position

(i) Relating the discussion of the application of the principle of collection limitation to the Section 69 of the IT Act is completely unwarranted as the Section deals with the lawful interception further to national security interests, defence, public order etc. Predictably, the Report fails to take note of the broad exceptions for national security, public security, defence, important economic or financial interest of a Member of the EU as contained in Article 13 of the EU Directive.

(ii) Evaluating the scope of privacy principle 'collection limitation' should explore the legal provisions with respect to the collection of personal information

(iii) Rule 5 (1) and (2) of the Privacy Rules address the requirements of this privacy principle obligating companies to take consent for the purpose of usage before collection of information. It also stipulates that the information collected should be for the lawful purpose, and collected if the information is necessary for the purpose.

7.4. Content Principles, 'Data quality and proportionality principles – Deletion / preservation of data

The report, while assessing the state against the principle, delves into section 67C that deals with the preservation of the information by intermediary. It makes the following observations;

(i) At present, India does not have any requirements that personal data should be de-identified or destroyed after its retention is no longer necessary according to the legitimate purposes for retaining it. WP 12 does not explicitly mention deletion or de-identification as a requirement for adequacy, unlike Article 6(1)(e) of the Directive which requires information to be kept in identifiable form 'no longer than is necessary'.

… Page 51 of the 2010 Report

India's position

(i) Evaluation of the provisions of section 67C against the principle is unwarranted as it deals with the responsibilities of an industry sector which falls into category of telecom/network service providers, hosting service providers, web portals, etc. It stipulates requirements for preserving the traffic information from the perspective of cyber offenses. The application of the principle should be assessed in the context of collection and processing of personal information.

(ii) Rule 5 (4) of the Privacy Rules states that sensitive personal data or information shall not be retained for longer than required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. This Rule now addresses the expectations as required by the privacy principle of 'deletion/preservation'.

7.5. Content Principles, Transparency

The 2010 Report made its observations against the principle as follows:

(i) *The IT Act 2000 does not impose obligations on private sector organizations to disclose details of their practices.*

(ii) *It further states that the absence of any similar principle governing the private sector means that Indian law does not provide adequate protection in respect to this point*

… Page 53 of the 2010 Report

India's position

(i) Rule 4 of the Privacy Rules embodies the principle of transparency in relation to collection and processing of personal information of data subjects. Rule 4 requires entities to maintain 'clear and easily accessible statements of its practices and policies' in the public domain so as to be easily available to the providers of information.

(ii) Rule 4 also requires entities to publish the privacy policy on the website of the company so as to be transparent to the data subjects about the specific type of information being collected, the purpose of collection, in the agency which is collecting and retaining the information on behalf of body corporates, rules relating to disclosure of information and reasonable security practices and procedures being implemented to protect such information.

7.6. Content Principles, Security

The 2010 Report explored the provisions of IT Act, and their relevance to the content principle. It has made the following observations:

(i) *Definition of body corporate excludes religious and social organization whose activities are not classified as 'commercial'. It also excludes the public sector.*

(ii) *No security standard has yet been prescribed by government.*

(iii) *There is significant protection in Indian law against third parties whose actions damage, destroy or disclose personal information. But these provisions do not apply to data controllers or service providers, who are the parties at whom the WP12 security obligations are aimed.*

(iv) *Section 84-A talks about encryption, but encryption policy has not yet been defined.*

(v) *B2B scenario is not addressed, as the provision of the Section 43 A excludes the parties that are in the lawful agreement.*

(vi) *India does not therefore provide an adequate level of security protections to personal information in either its public or private sectors*.

…Page 58-59 of the 2010 Report

India's position

(i) These observations reflect the situation prior to the notification of the Privacy Rules.

(ii) Rule 8 of section 43A details 'Reasonable Security Practices and Procedures'. It demands the companies to have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures.

(iii) Rule 8 also stipulates that in the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures.

(iv) It asks the entities to implement either IS/ISO/IEC 27001 or industry defined code of practice.

(v) Although the Privacy Rules define 'Reasonable Security Practices and Procedures' with reference to 'an agreement between the parties', it is important to mention that the Privacy Rules reflect the Government of India's benchmark of reasonable security practices and procedures and may be used for guidance in case of any such agreement deviating from standards notified by the Government as provided under Rule 8.

(vi) B2B transactions, in the era of globalization, tend to create jurisdictional issues with respect to enforcement of security and privacy. Enforcement of local laws on the transactions, where information security standards are primarily defined by a contract between the two parties, and one party is not under that jurisdiction of the country, may lead to questions relating to applicable law. Section 43A has been clearly drafted keeping this in mind. It doesn't relieve the controller/processor of information from information security obligations in a blanket manner.

(vii) With respect to encryption, the Department of Information Technology is in the process of notifying an encryption policy designed to significantly address information security concerns of businesses and consumers alike.

7.7. Content Principles, Onward transfer

In respect of this principle, the report made the following observations:

(i) There are no specific Indian laws restricting the transfer of personal data out of India.

(ii) Indian law does not provide adequate protection against onward transfers.

…Page 60 of the 2010 Report

India's position

(i) These observations reflect the situation prior to the notification Privacy Rules, which has brought the rule 7 stipulating conditions for transfer of data from India to third countries.

(ii) Rule 7, which is applicable even where there is no direct agreement between the provider and collector of information, would now ensure that sensitive personal data or information is only transferred to a country which provides the same level of data protection that is adhered to by the collector as provided for under the Rules. Further, the transfer may be allowed only for the performance of the lawful contract and when the provider of information has given a prior consent to data transfer.

7.8. Content Principles, Rights of Data Subjects (Access, rectification and opposition)

… Page 61-64 of the 2010 Report

The observations presented by the report and corresponding position are explained below:

(i) Informing of Data Subjects at the time of collection

India's position:

Rule 4 (1) and Rule 5 (2), 5 (6) and 5 (7) of the Privacy Rules stipulate requirements of intimating (providing notice), publishing policies, and making practices transparent to the data subjects.

(ii) Right of Access and Correction

India's position:

Rule 5(6) requires companies to permit the data subjects to review the information they had provided and ensure that information, if found to be inaccurate or deficient, is corrected or amended as feasible.

(iii) *Right to oppose processing*

India's position:

Rule 5(7) provides that data subjects have an option to withdraw their consent.

8. Additional Principles

The discussions, arguments, observations and India's current position with respect to the content principles are as follows:

8.1. Additional Principles, Sensitive Data

In respect of Sensitive Data, the report made its observations as follows:

(i) *No special protection in Indian law for sensitive personal information, other than s43A IT Act 2000 (when it becomes effective), and some very specific provision (s67 and s66E)*

(ii) *'Sensitive personal information' under s43A of the IT Act 2000, and the as-yet-undetermined definition of 'sensitive personal information*

(iii) *India does not yet provide an adequate level of additional protections for sensitive personal data*

… Page 65 of the 2010 Report

India's position

(i) Rule 3 under section 43A defined a set of data as sensitive personal information or data and entire set of Rules from Rule 4 to 8 have been enacted to ensure protection of sensitive information or data.

(ii) Rule 2 (1) (i) defines 'personal information' as information capable of identifying a person and Rule 3 has defined 'Sensitive Personal Data or Information' as identifiable information such as passwords, financial information physical, physiological and mental health condition, sexual orientation, medical records and history, biometric information etc. This is consistent with Article 2 (a) of the EU Directive which defines 'personal information' as any 'information relating to an identified or identifiable natural person' or 'in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

(iii) The basis of Section 43A has been designed to provide protection to the citizens in respect of collecting and processing their sensitive information

8.2. Additional Principles, Direct Marketing

In respect of Direct Marketing, the report made its observations as follows:

(i) *In relation to telemarketing, India now provides adequate protection to the right to opt-out from direct marketing.*

(ii) *In relation to other forms of direct marketing, by post ('snail mail') or via Internet (SPAM), India does not yet provide adequate protection.*

… Page 68 of the 2010 Report

India's position

(i) The data subject can take strength for their privacy protection from the Privacy rules: explicit consent for the defined purpose, collection limited to the purpose specified, withdrawal of consent for seeking protection against direct marketing

(ii) Rule 66A (c) inserted by the 2008 Amendment now provides specific protection against unsolicited commercial e-mails by specifying that any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages by making it a punishable offence.

8.3. Additional Principles, Automated Decisions

In respect of Direct Marketing, the report made its comment as 'Neither the Safe Harbor Agreement nor Canadian data protection legislation makes specific provision for such rights, yet both regimes have been deemed adequate'. However, the report observed that India does not provide adequate protection on this point.

… Page 69 of the 2010 Report

India's position

(i) As this point is not a hindrance for granting the adequacy status, as demonstrated by the US and Canada cases, it should not affect India's prospects for adequacy.

9. Adequacy Assessment: Procedural and Enforcement Mechanism

The adequacy assessment process looks at the procedural and enforcement primarily from five perspectives (i) Independence and functions of supervisory authorities (ii) Role of courts (iii) Provision of appropriate redress to the injured parties (iv) Delivery of a good level of compliance (v) Provision of support and help to individual data subjects

9.1. *Independence and functions of supervisory authorities*

In this regard, the 2010 Report evaluated the role of adjudicating officer and the cyber appellate tribunal. It made its observations as follows:

(i) The Cyber Appellate Tribunal and AO might possibly demonstrate independence over time, but it is too early to tell, and at present they have no role at all to play in relation to data protection.

(ii) Indian law provides very few data protection rights. Insofar as it does provide some limited rights, the independence of the supervisory bodies which administer and enforce those rights needs to be assessed in each case.

(iii) India's courts do have the necessary degree of independence for a supervisory body, but do not have a role in administering data protection rights generally.

… Page 85 of the 2010 Report

India's position

(i) The Adjudicating Officer is the 'First Court of Adjudication' and thus plays a very important link in the entire judicial process. His quasi-judicial authority covers not only the entire range of computer-related contraventions, especially under section 43, but also includes adjudging of body corporates vis-à-vis any failure to protect sensitive personal data.

(ii) Jurisdiction of Adjudicating Officer over all body corporates for the sections related to sensitive personal information, privacy policy and principles and reasonable security practices. The role of Adjudicating Officer is legally established with authority to impose fine; As per section 46(5) of the IT Act, he has powers of a civil court, i.e., all proceedings before the Adjudicating Officer are deemed as judicial proceedings.

(iii) The Act provides for the following quasi-judicial powers to the Adjudicating Officers:

a. To exercise jurisdiction in respect of the contraventions in relation to Chapter IX [Penalties and Adjudication] of the Act;
b. To receive a complaint from the complainant;
c. To issue notices together with all the documents to all the necessary parties to the proceedings, fixing a date and time for further proceedings;
d. To hold an inquiry or dismiss the matter or may get the matter investigated;
e. To enforce the attendance of any person or persons;
f. To fix a date and time for production of documents (including electronic records) or evidence; and
g. To hear and decide every application, as far as possible, in four months and the whole matter in six months.

(iv) IT Secretary of each state and union territories of India has been designated as Adjudicating officer ensuring the distribution of the function to support across the geographical areas covering billion plus population.

(v) Rule 5 (9) also provides an effective remedy to providers of information to address their grievances with respect to processing of information in a time bound manner. All organisations are bound to designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer is also required to redress the grievances or provider of information expeditiously within one month from the date of receipt of grievance.

9.2. Role of courts

In this regard, the 2010 Report made its observations as below:

(i) *Indian law provides few legal rights in relation to data protection, so there is limited scope in which the courts can act, and it is necessary to examine each situation to determine the role of the courts.*

(ii) *There is no recognized general right of action equivalent to data protection rights in the original jurisdiction of the Courts.*

(iii) *Access to the courts is therefore generally a positive feature of India's limited data protection rights. However, the limited nature of those rights means that Indian law does not, overall, provide an adequate level of protection in relation to the role of the Courts.*

… Page 88 of the 2010 Report

India's Position

(i) With the content principles matching the EU requirements, obligations of the body corporate stated, provisions on both civil and criminal offenses, the liability for failure to protect privacy, this point gets significantly addressed.

9.3. Provision of appropriate redress to the injured parties

In the regard the 2010 Report made its observation as follows:

(i) *Article 32 of the Indian Constitution provides very extensive powers to the Supreme Court to enforce constitutional rights, but they do not include a right to obtain compensation.*

… Page 90 of the 2010 Report

India's position

(i) Section 43A provides that entities possessing, dealing or handling any sensitive personal data or information are liable for damages by way of compensation if such entities are negligent in implementing and maintaining reasonable security practices and procedures thereby causing wrongful loss or wrongful gain to any person. This provision provides no limitation on the amount of compensation which may be provided to an injured party.

9.4. Delivery of a good level of compliance

In addition, by stating that Article 32 of the Indian Constitution does not include a right to compensation, the Report is factually incorrect in ignoring the plethora of case laws decided by the Supreme Court which have built the groundwork for compensatory jurisprudence. *In the regard, the* 2010 Report made its observation as follows:

(i) *Overall, India's data protection mechanisms (insofar as they exist) do not yet deliver a good level of compliance, with the exception of the right to access personal data in the public sector.*

(ii) *It is generally too early to tell whether those enforcement mechanisms actually deliver a good level of compliance - or whether there is a good level of voluntary compliance – because the legislation has not yet begun to operate (as in the case of s43A of the IT Act), or because there are no cases reported in its early stages of operation.*

… Page 91 of the 2010 Report

India's position

(i) The position has changed with the Privacy Rules and with the obligation of the entities to define their privacy policy, implement privacy principles, definition of reasonable security practices, requirement of establishing a security program, expectations to implement measures for the security of personal information, compensation provided for failure to protect information and a condition of the yearly audit of security practices, it may be argued that Indian data protection laws deliver a good level of compliance.

9.5. Provision of support and help to individual data subjects

In the regard, the 2010 Report made its observation as follows:

(i) There is no data protection office to advise data subjects on any aspect of data protection rights, or assist them to pursue their claims

(ii) Overall, supervisory bodies in India do not systematically advise data subjects on their data protection rights (insofar as they exist) or assist them to pursue their claims, with the exception of the right to access personal data in the public sector

… Page 92 of the 2010 Report

India's position:

(i) The role of Adjudicating Officer establishes a kind of administrative and supervisory office with an adequate level of empowerment. The adjudicating officers are increasingly adjudicating over the matters of data protection.

(ii) Further, the designation of a Grievance Officer under Rule 5 (9) provides an effective remedy to providers of information to address their grievances with respect to processing of information in a time bound manner.

10. Other perspectives

The adequacy assessment also takes a close look at all the contemporary developments in a country that have a bearing on privacy protection. The identity information, primarily due to the UIDAI project, and NATGRID as it is poised to access transaction information from the perspective of national security, seem to have attracted attention in the earlier study performed by the EU.

10.1. Identity Information

The 2010 Report took a note of concerns around the UIDAI project expressed as 'two main themes: the potential use of the database by the State for repressive and undemocratic ends; and the monetization of the database for private profit.

The Directive directs governments to "determine the conditions under which a national identification number or any other identifier of general application may be processed" (Art. 8(7). It expects that a privacy legislation for that system, or general data protection legislation.

India's Position

(i) UIDAI has drafted the 'National Identification Authority Bill', which is designed to take care of privacy concerns emanating from the UIDAI project. The Bill is in parliament now.

10.2. NATGRID

Data matching has not been a major method of social administration or business in India until now. However, as discussed in the previous section, the introduction of the ID number and the proposed developments of the NPR, National Citizenship Register, ID card, NATGRID, are likely (even if not all go ahead) to make it far easier (technically and socially) for Indian government agencies and companies to undertake data matching on a much more massive scale than in the past.

It further notes that whether the data protection aspects of these potential development will be addressed in a way which does not contradict necessary elements for adequate data protection remains to be seen, but is a very serious question given their scope. Much will depend in the short term on how the legal regulation of the ID number system develops.

India's Position:

(i) NATGRID has been envisaged to address the law enforcement and national security concerns. NATGRID project aims to facilitate information sharing among law enforcement agencies to combat terror threats.

(ii) The initiatives stemmed from the national security and defence concerns may not have any significance to adequacy discussion.

10.3. Publicly Accessible Data ('Public Registers')

The Article 29 Working Party did not single out public registers as one of the special types of processing relevant to adequacy assessments, but it is one of the types of processing specifically addressed by the Directive. The lack of controls over the creation of public registers in India, or the application of any privacy protections to them, must therefore be considered as a factor not favorable to the adequacy of India's data protection, though not a major factor.

India's Position:

(i) It may not be a major factor in the discussion of adequacy.

11. Adequacy Conclusions

The reports concludes with key following observations:

(i) *India does not at present provide adequate protection to personal data in relation to all sectors, or to the whole of its private sector or to the whole of its public sector. Nor does it provide adequate protection in any identifiable sub-sector.*

(ii) *None of the content principles identified by the Art. 29 Working Party as essential to adequacy are implemented in relation to the whole of the private sector and the public sector*

(iii) *On a more positive note, some aspects of the independence, powers and available remedies of some Indian supervisory bodies would contribute to a positive assessment of adequate protection if (as is not the case) they were administering adequately broad sets of principles. This is particularly so of the Information Commissions administering the RTI Acts, though they might not be able to exercise all of the required functions of a supervisory body (eg assistance to data subjects) even if the RTI laws contained a full set of data protection rights*

(iv) There is as yet no significant self-regulation for the purposes of data protection exercisable by data subjects in India. The self-regulation provided by DSCI is for the benefit of overseas companies outsourcing processing to India, and exercisable by them, not by data subjects.

(v) Overall, India as yet has not implemented data protection, though it is starting to take steps to do so.

… Page 93 of the 2010 Report

India's position

India's constitution, judicial precedences, courts proactive approach and rulings, legal advancements and evolving enforcement mechanisms are contributing to the ecosystem for a strong data protection regime in the country. Specific steps that have been undertaken recently close the gaps in terms of the content principles, procedural/enforcement mechanism, support system for citizens and obligations of companies for privacy protection. The changed scenario, as summarized in the following points, presents a strong case for arguing in favour of a positive assessment of Indian data protection regime.

(i) Indian constitution enshrines and promotes the modern value system through its commitment to fundamental rights of the citizen. It guarantees a set of personal rights to life, defined in a manner that are relevant irrespective of technological transformations. The law making process is taking a note of the societal and technological transformations to evolve sensible policies that reiterate meanings of personal rights in the technology driven era. Indian constitution provides the strength for legal, judicial and executive arrangements for protection of personal rights

(ii) Indian courts have been seen strong supporter of upholding personal rights and playing an important role in protecting the rights of individuals against excesses of the state. The role of the courts is a significant and positive background factor towards creating a data protection regime in the country

(iii) The court rulings and interpretations involve state action, and therefore are protections against the state, covering public sector organizations and government departments

(iv) The amendment of the IT Act, and the rules bring the private sector and public sector (except government departments) under the fold of a strong data protection regime

(v) Rules defined under the IT Act, section 43 A, bring content for data protection by defining privacy principles such as: 'Notice', 'Collection Limitation', 'Consent', 'Purpose & Use Limitation', 'Retention Limitation', 'Review & Access', 'Security', 'Transparency', and 'Onward Transfer',

(vi) The quasi judicial mechanism of Adjudicating Officer, distributed across the Indian states and union territories, role of civil courts, protection against criminal offenses such as identity theft, and removal of the cap on the liability for unauthorized access and privacy violation, significantly enhance the level data protection.

(vii) With provision of awarding compensation for failure to implement reasonable security practices - Rs 5 Crore (US$ 1.2 million) within the power of Adjudicating Officer, the concerns with respect to support to the data subjects are significantly addressed. The providers of information (data subjects) can also approach civil court if compensation desired is more than Rs 5 Crore (US$ 1.2 million).

(viii) The obligations of the companies to define their privacy policy, implement privacy principles, definition of reasonable security practices, requirement of establishing a security program, expectations to implement measures for the security of personal information, compensation defined for failure to protect information and a condition of the yearly audit of security practices set a level of compliance for for data protection

(ix) Data Security Council of India has been, with support of NASSCOM, is instrumental in bringing a strong data protection regime in the country. It is closely working with the government of India and its different functions in order to address policy issues. On the other hand, it has been takin all necessary steps in terms of developing security and privacy framework, and promoting implementation of privacy in the Indian industry. It is moving towards notifieying its assessment framework, which will be used for certification of privacy practices in the direction of establishing a self regulatory organization. The Indian industry shows a strong resolve to the cause of data protection by extending full support to the Data Security Council of India.

DATA SECURITY COUNCIL OF INDIA

A NASSCOM® Initiative

L: Niryat Bhawan, 3rd Floor, Rao Tula Ram Marg, New Delhi - 110057, India
P: +91-11-26155071 | F: +91-11-26155070 | E: info@dsci.in | W: www.dsci.in