Justice Ajit Prakash Shah
Former Chief Justice
High Court of Delhi

Dated: 16th October, 2012

Dear Dr. Ashwani Kumar Ji,

I am pleased to enclose the report of the **Group of Experts on Privacy** constituted by the Planning Commission under my chairmanship. The report covers international privacy principles, national privacy principles, rationale and emerging issues along with an analysis of relevant legislations/Bills from a privacy perspective. On the basis of deliberations and in depth analysis, the group has identified a set of recommendations, which the government may like to consider while formulating the proposed framework for a Privacy Act.

With warm regards,

A.P.Shah

(Ajit Prakash Shah)

Encl: Report of the Group of Experts on Privacy

Dr. Ashwani Kumar
MOS (Planning, S & T and Earth Sciences)
Planning Commission
Yojana Bhawan,
New Delhi – 110 001

Delhi Res. : F-6/A, Hauz Khas Enclave, New Delhi – 110016. Tel.: 011-26868687, Mobile : 9910160007
Mumbai Res. : 9-B, Samata, General Jagannath Bhosle Marg, Mumbai – 400 021 Tel.: 022-22831216
E-mail: ajitprakashshah@gmail.com

Report of the Group of Experts on Privacy

(Chaired by Justice A P Shah, Former Chief Justice, Delhi High Court)

Government of India
Planning Commission

Table of Contents

Executive Summary

I. With the initiation of national programmes like Unique Identification number, NATGRID, CCTNS, RSYB, DNA profiling, Reproductive Rights of Women, Privileged communications and brain mapping, most of which will be implemented through ICT platforms, and increased collection of citizen information by the government, concerns have emerged on their impact on the privacy of persons. Information is, for instance, beginning to be collected on a regular basis through statutory requirements and through e-governance projects. This information ranges from data related to: health, travel, taxes, religion, education, financial status, employment, disability, living situation, welfare status, citizenship status, marriage status, crime record etc. At the moment there is no overarching policy speaking to the collection of information by the government. This has led to ambiguity over who is allowed to collect data, what data can be collected, what are the rights of the individual, and how the right to privacy will be protected The extent of personal information being held by various service providers, and especially the enhanced potential for convergence that digitization carries with it is a matter that raises issues about privacy.

II. Global data flows, today, are no longer the result of a file transfer that was initiated by an individual's action for point-to-point transfer over 30 years ago. As soon as a transaction is initiated on the Internet, multiple data flows take place simultaneously, via phenomena such as web 2.0, online social networking, search engine, and cloud computing. This has led to ubiquity of data transfers over the Internet, and enhanced economic importance of data processing, with direct involvement of individuals in trans-border data flows. While this is exposing individuals to more privacy risks, it is also challenging businesses which are collecting the data directly entered by users, or through their actions without their knowledge, - e.g. web surfing, e-banking or e-commerce - and correlating the same through more advanced analytic tools to generate economic value out of data. The latter are accountable for data collection and its use, since data has become one of the drivers of the knowledge based society which is becoming even more critical to business than capital and labor. The private sector on the other hand, uses personal data to create new demands and build relationships for generating revenue from their services. The individuals are putting out their data on the web in return for useful services at almost no cost. But in this changed paradigm, private sector and the civil society have to build legal regimes and practices which are transparent and which inspire trust among individuals, and enhance their ability to control access to their data, even as economic value is generated out of such data collection and processing for all players. In order to understand these concerns and identify interventions for effectively addressing these issues, a brainstorming session on privacy-related issues was held in the Planning Commission under the chairmanship of Justice A P Shah, former Chief Justice of Delhi High Court. The meeting was presided over by Dr. Ashwani Kumar, MOS (Planning, S&T and MoES) and attended by representatives from industry, civil society NGOs, voluntary organizations and government departments.

III. During the meeting it was decided to constitute a small Group of Experts to identify key privacy issues and prepare a paper to facilitate authoring of the Privacy bill while keeping in view the international landscape of privacy laws, global data flows and predominant privacy concerns with rapid technological advancements. Accordingly a Group of Experts was constituted under the chairpersonship of Justice A P Shah. The

constitution and the terms of reference of the group is at Annex 1. The Group held several meetings to understand global privacy developments and challenges and to discuss privacy concerns relevant to India. The Group was divided into two sub-groups - one for reviewing privacy regimes around the world with a view to understand prevalent best practices relating to privacy regulation and the other for reviewing existing legislation and bills to identify prevalent privacy concerns in India. However, the committee did not "make an in-depth analysis of various programs being implemented by GOI from the point of view of their impact on privacy." This report, which is a result of the work of both sub-groups, proposes a detailed framework that serves as the conceptual foundation for the Privacy Act for India.

IV. This report proposes five salient features of such a framework:

1. **Technological Neutrality and Interoperability with International Standards:** The Group agreed that any proposed framework for privacy legislation must be technologically neutral and interoperable with international standards. Specifically, the Privacy Act should not make any reference to specific technologies and must be generic enough such that the principles and enforcement mechanisms remain adaptable to changes in society, the marketplace, technology, and the government. To do this it is important to closely harmonise the right to privacy with multiple international regimes, create trust and facilitate co-operation between national and international stakeholders and provide equal and adequate levels of protection to data processed inside India as well as outside it. In doing so, the framework should recognise that data has economic value, and that global data flows generate value for the individual as data creator, and for businesses that collect and process such data. Thus, one of the focuses of the framework should be on inspiring the trust of global clients and their end users, without compromising the interests of domestic customers in enhancing their privacy protection.

2. **Multi-Dimensional Privacy:** This report recognises the right to privacy in its multiple dimensions. A framework on the right to privacy in India must include privacy-related concerns around data protection on the internet and challenges emerging therefrom, appropriate protection from unauthorised interception, audio and video surveillance, use of personal identifiers, bodily privacy including DNA as well as physical privacy, which are crucial in establishing a national ethos for privacy protection, though the specific forms such protection will take must remain flexible to address new and emerging concerns.

3. **Horizontal Applicability:** The Group agreed that any proposed privacy legislation must apply both to the government as well as to the private sector. Given that the international trend is towards a set of unified norms governing both the private and public sector, and both sectors process large amounts of data in India, it is imperative to bring both within the purview of the proposed legislation.

4. **Conformity with Privacy Principles**: This report recommends nine fundamental Privacy Principles to form the bedrock of the proposed Privacy Act in India. These principles, drawn from best practices internationally, and adapted suitably to an Indian context, are intended to provide the baseline level of privacy protection to all individual data subjects. The fundamental philosophy underlining the principles is the need to hold the data controller accountable for the collection, processing and use to which the data is put thereby ensuring that the privacy of the data subject is guaranteed.

5. **Co-Regulatory Enforcement Regime:** This report recommends the establishment of the office of the Privacy Commissioner, both at the central and regional levels. The Privacy Commissioners shall be the primary authority for enforcement of the provisions of the Act. However, rather than prescribe a pure top-down approach to enforcement, this report recommends a system of co-regulation, with equal emphasis on Self-Regulating Organisations (SROs) being vested with the responsibility of autonomously ensuring compliance with the Act, subject to regular oversight by the Privacy Commissioners. The SROs, apart from possessing industry-specific knowledge, will also be better placed to create awareness about the right to privacy and explaining the sensitivities of privacy protection both within industry as well as to the public in respective sectors. This recommendation of a co-regulatory regime will not derogate from the powers of courts which will be available as a forum of last resort in case of persistent and unresolved violations of the Privacy Act.

Chapter 1: The Constitutional Basis for Privacy

1.1 Since the 1960s, the Indian judiciary, and the Supreme Court in particular, have dealt with the issue of privacy, both as a fundamental right under the Constitution and as a common law right. The common thread through all these judgments of the Indian judiciary has been to recognise a right to privacy, either as a fundamental right or a common law right, but to refrain from defining it in iron-clad terms. Instead the Courts have preferred to have it evolve on a case by case basis. As Justice Mathew put it, "The right to privacy will, therefore, necessarily, have to go through a process of case by case development." (Govind v. State of Madhya Pradesh, AIR 1975 SC 1378)

Right to privacy in the context of surveillance by the State

1.2 The very first case to lay down the contours of the right to privacy in India, was the case of *Kharak Singh* v. *State of Uttar Pradesh* (1964) SCR (1) 332, where a Supreme Court bench of seven judges was required to decide the constitutionality of certain police regulations which allowed the police to conduct domiciliary visits and surveillance of persons with a criminal record. The petitioner in this case had challenged the constitutionality of these regulations on the grounds that they violated his fundamental right to privacy under the 'personal liberty' clause of Article 21 of the Constitution. In this case a majority of the judges refused to interpret Article 21 to include within its ambit the right to privacy part the majority stated "The right of privacy is not a guaranteed right under our Constitution, and therefore the attempt to ascertain the movements of an individual is merely a manner in which privacy is invaded and is not an infringement of a fundamental right guaranteed in Part III." The majority however did recognise the common law right of citizens to enjoy the liberty of their houses and approved of the age old saying that a man's home was his castle. The majority therefore understood the term 'personal liberty' in Article 21 in the context of age old principles from common law while holding domiciliary visits to be unconstitutional. Two of the judges of the seven judge bench, however, saw the right to privacy as a part of Article 21, marking an early recognition of privacy as a fundamental right. Justice Subba Rao held "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."

1.3 The question of privacy as a fundamental right presented itself once again to the Supreme Court a few years later in the case of *Govind v. State of Madhya Pradesh* (AIR 1975 SC 1378). The petitioner in this case had challenged, as unconstitutional, certain police regulations on the grounds that the regulations violated his fundamental right to privacy. Although the issues were similar to the *Kharak Singh* case, the 3 judges hearing this particular case were more inclined to grant the right to privacy the status of a fundamental right. Justice Mathew stated:

> "Rights and freedoms of citizens are set forth in the Constitution in order to guarantee that the individual, his personality and those things stamped with his personality shall be free from official interference except where a reasonable basis for intrusion exists. 'Liberty against government' a phrase coined by Professor Corwin expresses this idea forcefully. In this sense, many of the fundamental rights of citizens can be described as contributing to the right to privacy."

1.4 This statement was however qualified with the disclaimer that this right was not an absolute right and that the same could be curtailed by the State provided it could establish a "*compelling public interest*" in this regard.

Balancing the 'right to privacy' against the 'right to free speech'

1.5 Subsequent to the *Govind* judgment, the Supreme Court was required to balance the right of privacy against the right to free speech in the case of *R. Rajagopal* v. *State of Tamil Nadu* (1994 SCC (6) 632). In this case, the petitioner was a Tamil newsmagazine which had sought directions from the Court to restrain the respondent State of Tamil Nadu and its officers to not interfere in the publication of the autobiography of a death row convict–'Auto Shankar' which contained details about the nexus between criminals and police officers. The Supreme Court framed the questions in these terms: "Whether a citizen of this country can prevent another person from writing his life story or biography? Does such unauthorised writing infringe the citizen's right to privacy? Whether the freedom of press guaranteed by Article 19(1) (a) entitles the press to publish such unauthorised account of a citizen's life and activities and if so to what extent and in what circumstances?"

1.6 While answering the above questions, a bench of two judges of the Supreme Court, for the first time, directly linked the right to privacy to Article 21 of the Constitution but at the same time excluded matters of public record from being protected under this 'Right to Privacy'. The Supreme Court held:

> "(1) the right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy. (2)The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."

The 'Right to Privacy' of HIV ('+'ve) patients

1.7 In the case of *Mr. 'X' v. Hospital 'Z'*, (AIR 1999 SC 495), the Supreme Court was required to discuss the scope of a blood donor's right to privacy of his medical records. The respondent hospital in this case had disclosed, without the permission of the blood donor, the fact that the blood donor was diagnosed as being a HIV patient. Due to this disclosure by the hospital, the lady who was to have been married to the blood donor had broken off her engagement and the donor was subject to social ostracism. Discussing the issue of privacy of medical records, the Supreme Court ruled that while medical records are considered to be private, doctors and hospitals could make exceptions in certain cases where the non-disclosure of medical information could endanger the lives of other citizens, in this case the wife.

Prior judicial sanction for tapping of telephones

1.8 In the case of *PUCL* v. *Union of India* ((1997) 1 SCC 30), the petitioner organisation had challenged the actions of the state in intercepting telephone calls. Recognising procedural lapses that had occurred, the court set out procedural safeguards which would have to be followed, even as it did not strike down the provision relating to interception in the Telegraph Act 1885. In arriving at its decision, the court observed: "Telephone-tapping is a serious invasion of an individual's privacy. It is no doubt correct that every government, howsoever democratic, exercises some degree of sub rosa operation as a part of its intelligence outfit, but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day." The court held: "Telephone-tapping would, thus, infract Article 21 of the Constitution of India unless it is permitted under the procedure established by law."The Supreme Court placed restrictions on the class of bureaucrats who could authorise such surveillance and also ordered the creation of a 'review committee' which would review all surveillance measures authorised under the Act.

The 'search and seizure' powers of revenue authorities

1.9 In 2005, the Supreme Court passed one of its most important privacy related judgments in the case of *District Registrar v. Canara Bank* ((2005) 1 SCC 496). In this case the Supreme Court was required to determine the constitutionality of a provision of the A.P. Stamps Act which allowed the Collector or 'any person' authorised by the Collector to enter any premises to conduct an inspection of any records, registers, books, documents in the custody of any public officer, if such inspection would result in discovery of fraud or omission of any duty payable to the Government. The main issue, in the case, related to the privacy of a customer's records stored by a financial institution such as a bank.

1.10 The impugned provision was held to be unconstitutional by the Supreme Court on the grounds that it failed the tests of reasonableness enshrined in Articles 14, 19 and 21 of the Constitution. The Court held that any legislation intruding on the personal liberty of a citizen (in this case the privacy of a citizen's financial records) must, in order to be constitutional, satisfy the triple test laid down by the Supreme Court in the case of *Maneka Gandhi* v. *Union of India.* This triple test requires any law intruding on the concept of 'personal liberty' under Art. 21, to meet certain standards:"(i) it must prescribe a procedure; (ii) the procedure must withstand the test of one or more of the fundamental rights conferred under Article 19 which may be applicable in a given situation; and (iii) it must also be liable to be tested with reference to Article 14." The impugned provision was held to have failed this test. More importantly, the Court ruled that the concept of privacy related to the citizen and not the place. The implication of such a statement was that it did not matter that the financial records were stored in a citizen's home or in a bank. As long as the financial records in question belonged to a citizen, those records would be protected under the citizen's right to privacy.

Privacy in the context of sexual identities

1.11 In the case of *Naz Foundation v. Union of India* (WP No. 7555 of 2011) the Delhi High Court 'read down' Section 377 of the Indian Penal Code, 1860 to de-criminalise a class of sexual relations between consenting adults. One of the critical arguments accepted by the Court in this case was that the right to privacy of a citizen's sexual relations, protected as it was under Article 21, could be intruded into by the State

only if the State was able to establish a compelling interest for such interference. Since the State was unable to prove a compelling state interest to interfere in the sexual relations of its citizens, the provision was read down to decriminalise all consensual sexual relations.

1.12 Privacy has emerged, and evolved, as a fundamental right through these various decisions of the courts.

Chapter 2: International Privacy Principles

Comparison of International Privacy Requirements

2.1.Different geographies across the globe have defined their privacy requirements, articulating the requirements for the protection of the personal data and prevent harm to an individual whose data is at stake. The following table represents the derivation of privacy requirements as articulated by the OECD Privacy Guidelines, EU Data Protection Directives, APEC Privacy Framework, Canada PIPEDA (Personal Information Protection and Electronic Documents Act), and Australia ANPP (Australia National Privacy Principles).

			OECD Guidelines	EU Data Protection	APEC Framework	Canada PIPEDA	Australia ANPP
Privacy Requirements	Accountability	Organization's accountability towards personal information	✓	✓	✓	✓	
	Notice	Notice in clear language for collection, policy notification	✓	✓	✓	✓	✓
	Consent	For collection and use	✓	✓	✓	✓	✓
	Collection Limitation	Restricting the collection to the identified purpose only	✓	✓	✓	✓	✓
	Use Limitation	Restricting the use for the stated purpose only	✓	✓	✓	✓	✓
	Disclosures	Terms to disclosure to third parties & any other reason			✓	✓	✓
	Access & Corrections	Individual's access to his info and update/ correct his info	✓	✓	✓	✓	✓
	Security/ Safeguards	To prevent loss, misuse, unauthorized access	✓	✓	✓	✓	✓
	Data Quality	To ensure info is accurate, complete & up-to-date	✓	✓	✓		✓
	Enforcement	Assurance over adherence to policies & Complaint resolution		✓	✓	✓	
	Openness	Policies clearly published & available	✓	✓	✓	✓	✓
Additional Requirements	Anonymity	De-identification of personal information					✓
	Transborder data flow	Personal data transfer across geographies	✓	✓	✓		
	Sensitivity	Specified inf that requires specific controls		✓			

2.2.Privacy Principles such as Notice, Consent, Collection Limitation, Use Limitation, Access and Corrections, Security/Safeguards, and Openness cut across these frameworks. The principle of Enforcement, which APEC calls as Preventing Harm, is introduced by APEC, EU and the Canadian privacy enforcement regimes. The EU Data Protection Directive, OECD Guidelines and APEC framework additionally deals with the subject of Trans-border data flow. Australia's ANPP specifically prescribes de-identification of the personal information.

Recent developments in privacy laws

2.3.The European Union (EU), the United States and the Organisation for Economic Co-operation and Development (OECD), Australia and Canada have debated changes to existing privacy regimes in the wake of technology and globalization challenges to privacy that have emerged over the last two decades. The key issues to emerge from these debates are:

EU Regulation of January 2012[i]:

2.4.Several new principles and changes to existing principles were suggested by the EU Regulation of January 2012. These include:

- More explicit expression of the **"data minimization" principle** and will require companies to limit the amount of data they collect much more strictly.[ii]
- **Accountability of data controllers** by requiring that personal data be processed under the responsibility and liability of the controller. The data controller is also responsible for compliance with the Regulation.[iii]
- **Right to object by the data subject for the sending of direct marketing**; Opt-in consent is, however, not required.[iv]
- Data controllers bear the **burden of proof** in showing that data subjects consented to the subject of personal data.[v]
- **Expands the definition of sensitive data** to also include genetic data and data concerning "criminal convictions of related security measures".[vi]
- **Right to be forgotten and to erasure:** Data must not be retained indefinitely and time limits must be set in place after which data must be erased from the system.[vii]
- Data controllers must have "**transparent and easily accessible policies** with regard to the processing of personal data and for the exercise of data subjects' rights"
- **Right to data portability** allowing individuals to change online service providers.[viii]
- **Regulate the use of "Profiling"[ix]**
- **Accountability of data controllers**, and independent verification of compliance measures.[x]
- Data controllers implement "appropriate technical and organisational measures" including **Privacy by Design**, and **Privacy by default**.[xi]
- Data controllers subjected to wide-ranging **data security obligations.[xii]**
- **Data breach notification requirement** applicable to all types of data controllers, notification of a data breach to be given by a data controller to both its Lead DPA and to the data subjects concerned.[xiii]
- **Data protection impact assessments** are to be carried out by data controllers and data processors.[xiv]
- **Data protection officers mandatory** for all public authorities and for all companies with more than 250 employees.[xv]
- The Regulation also foresees **drafting of codes of conduct covering various data protection sectors,** and allows them to be submitted to DPAs, which may give an opinion as to whether they are "in compliance with the Regulation".[xvi] Compliance with a code of conduct may be deemed to satisfy the legal requirements of the proposed Regulation. Article 39 establishing **"data protection certification mechanisms and of data protection seals and marks"**, is encouraged, though the legal effect of such recognition needs to be clarified.[xvii]

US Consumer Privacy Bill of Rights[xviii]

2.5.The US Consumer Privacy Bill of Rights states that consumers have a right to:

- Individual Control over what personal data companies collect and how they use it **(Consent, Notice/Choice**)[xix]
- Transparency through easily understandable and accessible information about privacy and security practices **(Transparency/Openness)**[xx]
- Respect for Context: that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data **(Use Limitation)**[xxi]
- Secure and responsible handling of personal data **(Security)**[xxii]
- Access and Accuracy: access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate **(Access and Correction)**[xxiii]
- Focused Collection: reasonable limits on the personal data that companies collect and retain **(Collection Limitation)**[xxiv]
- Accountability: personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights **(Accountability)**[xxv]

OECD Privacy Principles[xxvi]

2.6.The discussion on revision of OECD privacy principles has revolved around three topics: (1) The roles and responsibilities of key actors; (2) Geographic restrictions on data flows; and (3) Proactive implementation and enforcement.

1. Engage in efforts to educate and raise awareness of privacy risks and ways to mitigate them.By emphasizing transparency and individual consent, the current privacy framework imposes significant, sometimes unrealistic obligations on both businesses and individuals. On the one hand, businesses are expected to explain their data processing activities on increasingly small screens and seek consent from often-uninterested individuals; on the other hand, individuals are expected to understand complicated privacy disclosures and knowingly consent to them. It is not clear as to the role that consent should play in an age where data flows become increasingly complex, multiple parties are involved, and information is provided to individuals with short attention spans on increasingly small screens? What is the right balance between individual consent on the one hand and efficiency or legitimate business interests on the other hand
2. The OECD Privacy Guidelines have long recognized that consent is not the *sine qua non* of data processing. The "collection limitation principle", for example, states that "data should be obtained by lawful and fair means and, *where appropriate*, with the knowledge or consent of the data subject".
3. Proactive implementation and enforcement elaborate the accountability principle to feature concepts like privacy by design and data breach notification. Undertake analysis of the economics of remedies and sanctions by enforcement authorities, as well as trying to enhance international regulatory cooperation and interoperability of regulatory frameworks

APEC Privacy Framework[xxvii]

2.7.This is a grouping of some 21 countries that has come up with the APEC Privacy Framework to promote e-commerce. Self-regulation is part of the APEC Privacy Program, which has taken the approach of accountability under which the data protection obligations flow along with data in trans-border data flows. In order to accommodate different privacy laws in various countries, APEC has placed emphasis on the practical aspects of data flows, and on the manner of interface between various players including companies, regulators, and governments. **Cross-Border Privacy Rules (CBPRs)**, along with information sharing, investigation and enforcement across borders among regulators, including **self-regulatory organisations (SROs)** will form an integral part of the APEC Privacy Framework. The CBPRs are akin to Binding Corporate Rules (BCRs) allowed to Multinationals under the EU Directive.

Australia

2.8.The Australian Law Reform Commission produced an exhaustive three-volume report in May 2008 titled *For Your Information* ("ALRC Report") which recommended 11 UPPs to apply to both the private and the public sector.[xxviii] These are:

1. Anonymity and Pseudonymity
2. Collection
3. Notification
4. Openness
5. Use and Disclosure
6. Direct Marketing (applicable only to organisations)
7. Data Quality
8. Data Security
9. Access and Correction
10. Identifiers (applicable only to organisations)
11. Cross Border Data Flows

2.9.In response to these recommendations, and on this basis, the Australian government released an 'exposure draft' of **13 Australian Privacy Principles** (two additional principles are owing to the Access and Correction principles being made distinct and a separate principle protecting unsolicited information).[xxix] These principles represent a clear move by the Australian government to establish a streamlined and unified framework of principles applicable across the board ("to all entities"), designed to effectively protect the collection, holding use and disclosure of all personal information. In addition, these principles are technology neutral and thus are envisaged to be applicable to newer technologies that may develop over time and have privacy implications.

2.10. The principles are:

1. Open and Transparent Management of Personal Information

Principle 1 requires the incorporation of privacy safeguards before information is collected and stored by entities. It is an example of "privacy by design" in action which seeks to ensure that privacy and data protection are included in the design of information systems. The key significance of this principle is to institutionalise a culture of privacy protection in entities from the very outset, without waiting for a *post-facto* remedy to adequately take care of privacy concerns.

2. Anonymity and Pseudonymity

Principle 2 provides individuals the options of not identifying themselves or using a pseudonym while dealing with entities. Entities thus must consider whether it is *necessary* to require the specific identification asked for. The exception to the principle, narrowly construed, is when such non-identification is not lawful or practicable, i.e. where the law requires identification. This principle thus fits well with the principle of data minimisation that is generally considered desirable especially insofar as electronic data is concerned.

3. Collection of Solicited Personal Information

The necessity principle introduced by Principle 2 is extended in Principle 3 which lays down a functions test, i.e. unless certain personal information is *reasonably necessary* or directly related to the performance of one of the entity's functions or activities, it shall not be collected. This also extends to sensitive information which can only be collected by consent, unless it is related to war and warlike activities, diplomatic and consular processes and assisting in the location of missing persons. This principle represents a watered down version of the ALRC Report's recommendations, owing to the use of the word "reasonably" which mitigates the requirement of necessity thereby allowing the entities to collect personal information in a wider set of circumstances.

4. Receiving Unsolicited Personal Information

This principle applies only to unsolicited information which an agency may have *received.* The test that an entity in possession of such unsolicited information must use is the one laid down in Principle 3, i.e. whether it could have reasonably solicited the information. If it could, then the rest of the principles apply; if it could not, then this principle requires that the information be destroyed or de-identified. The key significance of this principle is to bring unsolicited personal information within the ambit of the Privacy Act.

5. Notification of the Collection of Personal Information

The notification principle requires the individual whose personal information is being collected to know why the information is being collected and the specific uses it is going to be put to. The exact aspects which have to be notified can be found in NPP 1.3 and 1.5 (existing Privacy Act). The rationale behind this provision is to ensure greater transparency in data handling thereby giving individuals greater information and consequently greater potential for control over use of their personal information.

6. Use or Disclosure of Personal Information

This principle sets out the circumstances in which entities may use or disclose personal information that has been collected or received. It is evident that it can be used for the primary purpose for which it has been collected; in case of secondary purposes, the general rule is that the information cannot be used unless there is consent. However, this principle also contains a long list of 'public policy' exceptions of when the consent criterion is overridden by public interest, such as when disclosure is required by law, necessary to save life, part of diplomatic and consular processes etc. The wide ambit of the exceptions has led to considerable concern regarding the sanctity of the principled statement itself.

7. Direct Marketing

Principle 7 regulates a specific purpose for use and disclosure of personal information, i.e. when such information is used to advertise or sell goods via direct marketing. It however excludes tele-marketing and direct marketing by electronic communication as they are covered under the Spam Act 2003 and the Do Not Call Register Act 2006. Insofar as other types of direct marketing are concerned, this principle makes a distinction between sensitive information which can only be used expressly with consent; for non-sensitive information, if the individual reasonably expects the information to be used for direct marketing and has an easy option for opting out, it can be so used; in all other cases, i.e. where information is not directly obtained from the individual, the obligations are onerous on the marketer. By setting out this threefold model, the principle dispenses with the earlier existing distinction between existing and potential customers of an entity, by bringing both under its fold. In addition, the extra emphasis placed as a result of this principle on direct marketing shows its increasing significance in affecting privacy in Australia, a trend with parallels across the world.

8. Cross Border Disclosure of Personal Information

Principle 8 incorporates the requirement of accountability in cross border data flows. As a result of this principle, Australian entities which may be sending data abroad for any reason will continue to remain liable in Australian law for actions taken by the foreign handler with regard to the data. Compliance with this principle usually takes the form of a contract between the Australian entity and the foreign data handler, the latter undertaking to comply with the privacy principles, despite itself not being a private entity. The only concern raised with regard to this principle is that when the Australian entity reasonably believes that the data protection regime in the foreign country in question is substantially similar or better and an individual has access to overseas enforcement mechanisms, it is not held accountable for the data handler's actions. This creates principled problems (too wide an exception to accountability) and policy ones (can be used in bundled consent to disclaim liability in a wide number of situations).

9. Adoption, Use or Disclosure of Government-related Identifiers

This principle lays down the significant rule that the scope for data matching by entities must be reduced to the extent possible. Government-related identifiers, i.e. a number, letter or symbols used by the government for identification (eg.) Unique ID, Tax File Number, Social Security Number etc.) cannot generally be used by organisations for their own identification purposes. The only exception is when such use is required or permitted by law or by regulations, provided the entity using such information is also expressly permitted to do so in the regulations. In addition, a separate sub-principle regulates use and disclosure of such information by entities. The key thrust of this principle is thus to ensure that government related identifiers used for particular social welfare purposes remain tethered to their original purpose and do not become facilitators of data matching across the private and public sectors, which has tremendous privacy implications.

10. Quality of Personal Information

This principle is aimed at ensuring the integrity of personal information. It is thus an obligation on all entities to ensure that the information they collect or use is accurate and up-to-date. This is necessary to prevent misinformation about an individual from spreading and thereby ensuring integrity and quality.

11. Security of Personal Information

There are twin aspects to this principle. First, the entity which holds personal information must ensure its security. This extends to both security of physical information as well as encryption or other forms of security for electronic information. At the same time, if the entity holds information about an individual which it no longer needs, then it must take steps to securely destroy or de-identify the information. Though the "right to be forgotten" is not expressly part of Australian law, this principle comes close to making it obligatory on entities to destroy information when it is not necessary, though when such an occasion arises is not clearly spelt out.

12. Access to Personal Information

This principle states that access to personal information must reasonably be provided to the individual. It must also be done speedily, within 30 days by a government agency (provided in the Principle) and within 15 days for straightforward requests and 30 days for more complex requests to private sector organisation (guidance issued by OPC). At the same time there is a long list of exceptions as to when access need not be provided. The key point to note in this regard is the interface between the Privacy Principles and the Freedom of Information Act under which several requests for access will be made and the crucial need to ensure that the two provisions do not contradict each other.

13. Correction of Personal Information

This principle is, most accurately, an extension of Principle 10 above which obliges entities to hold accurate information about individuals. When information is inaccurate or not up-to-date, and the entity is either asked to correct it (or to associate a statement that it is inaccurate) by the individual or discovers such inaccuracy itself, it is obliged to correct such wrongly held information (or associate a statement to the effect that it may be inaccurate) and notify third parties to whom it may have communicated the said information, within a reasonable period of time, free of charge. [xxx]

Canada

2.11. In Canada there is no single comprehensive law to privacy.[xxxi] Canada's legislative privacy regime consists of two horizontal legislations at the federal level, one which is applicable to the public known as the Privacy Act,[xxxii] and one to the private sector known as Personal Information Protection and Electronic Documents Act ("PIPEDA")[xxxiii]. Sectoral privacy legislations can be found at the federal and provincial level. For example: the Bank Act, the Insurance Companies Act, the Telecommunications Act, and the Young Offenders Act all address privacy at the federal sectoral level.[xxxiv]

PIPEDA[xxxv]:

2.12. In Canada the private sector is governed by the Personal Information Protection and Electronic Documents Act. PIPEDA was enacted with the purpose of balancing data subjects' right to privacy with the increasing need of organizations to collect, use and disclose personal information to a reasonable degree, and applies to all "organizations where personal information is collected, used or disclosed in the course of "commercial activities" except where provincial privacy law applies, and where personal information relates to the organization's employees and it collects, uses or discloses the data in connection with a federal undertaking or business. [xxxvi]

2.13. PIPEDA explicitly excludes the following from the scope of its application:

1. Government institutions to which the Privacy Act already applies;
2. Information collected, used or disclosed only for personal and domestic purposes; and
3. Information collected, used or disclosed only for journalistic, artistic or literary purposes.[xxxvii]

2.14. PIPEDA defines the term "personal information" as any information about an identifiable individual, other than the name, title or business address or telephone number of an employee of an organization.[xxxviii] The privacy principles found under PIPEDA are:

1. **Accountability**[xxxix]
   This principle requires that organizations take responsibility for personal information in their control. Organizations will designate individuals to ensure compliance. The designated individuals must make their identities available on request. The organization will retain responsibility for personal information where it transfers it to a third party for processing. It is recommended that a comparable degree of protection must apply to the information while it is being processed, through contract or otherwise

2. **Identifying Purposes**[xl]
   This principle requires that organization identify and document the purposes for which personal information is collected in order to comply with the Openness principle and the Individual Access principles. The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. When personal information that has been collected is to be used for a purpose not previously identified, the new purpose must be identified prior to use.

3. **Consent**[xli]
   This principle requires individual knowledge and consent, except where inappropriate, before personal information can be collected, used, or disclosed. An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal. Exceptions to this principle are enumerated in the Act.

4. **Limiting Collection**
   This principle requires that personal information can be collected only where it is necessary for identified purposes. Information should be collected by fair and lawful means.[xlii]

5. **Limiting use, disclosure, and retention**[xliii]
   This principle requires that personal information cannot be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of specified purposes. Organizations should develop guidelines and implement procedures with respect to the retention of personal information. Personal information that is no longer required to fulfill identified purposes should be destroyed, erased, or made anonymous. Organizations shall

develop guidelines and implement procedures to govern the destruction of personal information. Exceptions to this principle are enumerated in the Act.

6. **Accuracy**[xliv]
   This principle requires that personal information be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards**[xlv]
   This principle requires that physical, organizational, technical and/or other safeguards be taken to secure collected information, as necessary, given the sensitivity of the information. Specifically, safeguards against loss, theft, unauthorized access, disclosure, copying, use and modification must be put in place.
8. **Openness**[xlvi]
   This principle requires that the data subject is informed by organizations of the policies and practices that relate to the management of personal information, in a form that is easily understandable and available. Specifically, the information should include the following:
   1. Name or title, and address, of the person accountable for the organization's policies and practices, and to whom complaints or inquiries can be forwarded;
   2. Means by which to access personal information held;
   3. Description of the type of personal information held, along with a general account of its use;
   4. Information that explains the organization's policies, standards, or codes; and
   5. What personal information is made available to related organizations such as subsidiaries.

9. **Individual Access**[xlvii]
   This principle requires that if requested, an individual is informed of the existence, use, and disclosure of his or her personal information and be given access to that information. The reasons for denying access should be provided to the individual upon request. Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Exceptions to this principle are enumerated in the Act.

10. **Challenging Compliance**[xlviii]
    This principle requires that organizations investigate all complaints received. An individual shall be able to address a complaint concerning compliance with these principles to the designated individual(s) accountable for the organization's compliance. Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information.

The Privacy Act 1985 [xlix]

2.15. The Privacy Act came into force in 1985, with the stated purpose of preserving individuals' privacy in their personal information where it is held by the federal government or an agency thereof and to create a statutory right to access that

information.[l] The Act does not establish specific privacy principles, but does provide the following regulations:

1. **Accountability**
   Accountability of the Act rest with the "head" of a government institution as defined under section 3, or a designated Minister in the context of personal information and exemption banks. [li]

2. **Identifying Purposes**[lii]
   A government institution shall inform any individual from whom the institution collects personal information of the purpose for which the information is being collected. Exceptions to this principle are enumerated in the Act.

3. **Limiting Collection** [liii]
   Only personal information relating directly to an operating program or activity of a government institution can be collected.

4. **Limiting Use**[liv]
   Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution, except for the purposes for which it was obtained. Additional exceptions to this principle are enumerated in the Act.

5. **Accuracy/quality**[lv]
   A government institution must take all reasonable steps to ensure that personal information used for an administrative purpose is as accurate, up-to-date and complete as possible.

6. **Openness**[lvi]
   Every government institution must create an information bank that includes all personal information under the control of the government institution that has been used or is available for administrative purposes, or is organized or intended to be retrieved by the name of an individual or identifying number.[lvii]

   A designated Minister must cause to be published on an annual basis an index of
   - (i) all personal information banks,
   - (ii) the identification and description of the bank,
   - (iii) the name of the government institution that has control of the bank,
   - (iv) the title and address of the appropriate officer to whom requests relating to
   - (v) personal information in the bank should be sent to,
   - (vi) a statement of the purposes for which personal information in the bank was obtained,
   - (vii) a statement of the retention and disposal standards,
   - (viii) an indication, if applicable, that the bank was designated an exempt bank, and all classes of personal information under control of the government institution.

7. **Individual Access**[lviii]
   Canadian citizens or a permanent resident has a right to request access to:

1. Any personal information about the individual contained in a personal information bank; and
2. Any other personal information about the individual controlled by a government institution with respect to which s/he is able to specify the location of the information so it can be retrieved. Exceptions to this principle are enumerated in the Act.

8. Challenging Compliance [lix]

Individuals may file a complaint with the Commissioner if:

1. Personal information held by governmental institutions has been disclosed.
2. Individuals who have been refused information that was requested.
3. Individuals whose corrections to information were refused by the governmental institution.
4. Individuals who have not been given access to personal information in the language requested.
5. Individuals who have not been given access to personal information in an alternative format.
6. Individuals who have had to pay a fee that they consider inappropriate when accessing information.

Chapter 3: National Privacy Principles, Rationales, and Emerging Issues

3.1. The privacy principles represent the foundation for any regime to protect privacy. As demonstrated in the previous chapter, with regard to the principles in force the world over, there is a high degree of agreement among various approaches, most specifically, the principles followed by the US, OECD, EU and APEC, where transparency, enforcement and accountability are considered the cornerstone for privacy protection. While there are minor variations between these various formulations, it would not be inaccurate to suggest that there is a set of globally accepted privacy principles. On this basis, a set of National Privacy Principles can be enumerated as the distillation of global best practices which can be effectively implemented in Indian conditions. The principles must establish:

(1) Safeguards and procedures over the collection, processing, storage, retention, access, disclosure, destruction, and anonymization of sensitive personal information, personal identifiable information, sharing, transfer, and identifiable information.

(2) Rights of the data subject in relation to their Sensitive Personal Information, Personal Identifiable Information, and Identifiable Information.

The principles will place an obligation on all public and private data controllers to put in place safeguards and procedures that will enable and ensure these protections and rights. The principles must be applicable to any information concerning an identified or identifiable natural person. Existing and emerging legislation, practices, and procedures should be brought into compliance with the National Privacy Principles.

Alongside the National Privacy Principles, self-regulating bodies will have the option of developing industry specific privacy standards that would be in conformity with the National Privacy Principles, which should be approved by a Privacy Commissioner. The Privacy Commissioner should have the power to enforce the agreed-upon standards, thus creating a system of co-regulation. If SROs do not develop standards, their member organisations shall be required to adhere to the National Privacy Principles.

3.2. The proposed privacy principles are the following:

Principle 1: Notice

Principle: A data controller shall give simple-to-understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:

a) **During Collection**

- What personal information is being collected;
- Purposes for which personal information is being collected;
- Uses of collected personal information;
- Whether or not personal information may be disclosed to third persons;
- Security safeguards established by the data controller in relation to the personal information;

- Processes available to data subjects to access and correct their own personal information;
- Contact details of the privacy officers and SRO ombudsmen for filing complaints.

b) **Other Notices**

- Data breaches must be notified to affected individuals and the commissioner when applicable.
- Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.
- Individuals must be notified of changes in the data controller's privacy policy.
- Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.

Rationale: The notice principle ensures that individuals are informed of how their information will be used, allows data controllers to communicate their intents and practices to data subjects and other stakeholders, and allows the individual to hold the data controller accountable to the practices articulated in the notice.

Issues and Developments:

- Notice together with other user centric principles such as choice and consent have been used to transfer obligations for protecting privacy to data subjects.
- Notices displayed are complex, lengthy, difficult to understand, non-transparent – making it difficult for the data subjects to understand the implications of data sharing.
- Acceptance / Reading of a notice is used to take consent without giving data subjects any meaningful choice to consent.

Given the above issues, it is recommended that the organisation should have simple, short and easy notices and the notice principle along with choice and consent principles should not be used to transfer an organisation's privacy obligations to data subjects.

Principle 2: Choice and Consent

Principle: A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. The data subject shall, at any time while availing the services or otherwise, also have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which the said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.

When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required.

Rationale: The choice and informed consent principle empowers the individual to approve and authorise collection and usage of personal information for defined purposes. The principle ensures that data controllers provide simple choices to data subjects that allow them to make informed decisions about the extent to which they would like to share their personal information, prior to collecting that information. When individuals are mandated by law to share information, the principle ensures that this is done in accordance with the other National Privacy Principles, and that the information, if shared in public databases, is not retained in an identifiable form longer than is necessary.

Issues and Developments:

- Data subjects are limited in their ability to exercise control over the ways organisations use their personal information once it has been disclosed.
- Data subjects are 'forced' to give their consent without being given any meaningful choices – they are denied services if they do not agree with the privacy terms and conditions of the organisation.
- Implicit consent is taken from data subjects without their full understanding of privacy implications.
- In an online environment, the way mechanisms to provide choices are positioned, it becomes difficult for the data subjects to locate and exercise their choice. Practical difficulties in consent withdrawal and choice limitation once the information has been shared exist.
- From a business perspective, it may be irrelevant, and operationally difficult to provide choices and / or take consent in every type of service it offers. Many services the organisation offers may not be required to provide choice and / or take consent. From a data subject perspective, data subjects may not like to be offered choices or provide consent for every transaction as it may adversely impact their user experience when dealing with organisations.
- From online services perspective, many services such as email, social networking, etc. are offered for 'free' to the data subjects. The organisations offering such services use the collected personal information to generate revenue through advertising, etc. These are emerging issues in the privacy arena.
- From an Indian context, integration of illiterate and poor residents in the overall privacy design especially in the implementation of user centric principles is a major challenge.

Given the above issues, it is advised that there should be criteria to decide when to give choice and take consent. All transactions may not require the organisation to provide choice and take consent. As mentioned in the notice principle, user centric principles such as choice and consent principles should not be used to transfer organisation's privacy obligations to data subjects, instead the organisation should take responsibility for protecting privacy. Also, it is important from the Indian context that when executing choice and consent principle (also applicable for access and correction), organisations take into consideration the needs of citizens who are poor, illiterate, etc. Separately, due care also needs to be taken for children, differently abled citizens, etc. Additionally, the consent seeking operations must seek active and positive user actions. Many organisations try to opt deceiving, and negative methods for seeking the consent. The Choice and Consent principle is intended to give control to data subjects over their personal information during collection and while it is in the custody of the organisations.

Principle 3: Collection Limitation

Principle: A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

Rationale: The collection limitation principle ensures that data controllers only collect personal information that is necessary for achieving the stated objective, and that all collection is lawful and fair. This reduces the probability of misuse of individuals' personal information.

Issues and Developments: Because of advancements in technology, organisations collect data through automated mechanisms such as cookies, web beacons, etc. without the knowledge of the data subject. This is more relevant in an online environment. Also, organisations correlate data subjects' profile with other available third party sources to build a more comprehensive data profile of data subjects without their knowledge. Increasing involvement of multiple third parties in data collection increases the chances of additional data collection which may be of direct / indirect benefit to the third parties. Another concept of **data minimization** is also being discussed, which is intended to minimize the data subjects' personal information dealt with by organisations by limiting collection and retention. This concept can be subsumed under the Collection Limitation principle.

Principle 4: Purpose Limitation

Principle: Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

Rationale: The purpose limitation principle ensures that personal information is used only in compliance with the National Privacy Principles and only for intended and agreed purposes. The principle also ensures that personal information is retained by the data controller only as long as is necessary to fulfill the stated purposes, and is destroyed in accordance with identified procedures when it is no longer required.

Issues and Developments: Because of globalization, the concept of extended organisation and proliferation of technology especially through the Internet, personal information collected is shared with multiple third parties across the globe. In such a scenario implementing use limitation principle especially in the context of retention becomes very difficult. Ascertaining that all the parties having the custody of the personal information do not retain the personal information beyond the necessary time frame is difficult. It is a huge challenge for the organisation, to which data was originally submitted, to track the information flow and its usage across the entire supply chain. To strengthen the data subject's right the new EU privacy regulation proposal has added a new principle- the **right to be forgotten** (which gets covered under the retention aspect of

use limitation principle**),** however its implementation seems difficult given the environment in which personal information is processed today.

Principle 5: Access and Correction

Principle: Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data . Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Rationale: The access and correction principle ensures that data controllers provide access mechanisms to data subjects for inquiring if a data controller is holding their personal data, and for viewing, modifying and deleting their personal information.

Issues and Developments: Data subjects are limited in their ability to exercise control over the ways organisations use their personal information once it has been disclosed. Data subjects are not provided access to certain categories of data especially those collected from automated techniques or indirect sources. In case any organisation (not the data controller) holds any personal information about the data subject and uses this information to reach out to the data subject, the data subject does not have the legal authority to know how this organisation got his / her data. Such organisations do not act transparently in providing the data subject the required information.

Principle 6: Disclosure of Information

Principle: A data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Rationale: The disclosure to third parties principle ensures that data subjects are informed and consent taken [except when an exemption exists] when their personal information is transferred to third parties. The principle requires data controllers ensure that third parties also adhere to the National Privacy Principles. The principle also ensures that any disclosure by the data controller to a third party that has been authorized and is a governmental agency is in compliance with the National Privacy Principles. Furthermore the principle makes any de-anonymization of information that was anonymised/aggregate information for the transfer a violation of the principle.

Issues and Developments: There is lack of visibility over involvement of third parties vis-à-vis transaction of personal information. It is difficult to keep a check on third parties vis-à-vis use of personal information. It is difficult to ascertain that third parties especially after termination of services dispose the personal information in their custody. There are huge compliance costs for both the organisations (data controllers) and third parties because of multiple audits and assessments. Given the above challenges, the laws around the world are increasingly extending the responsibility of protecting information being

disclosed to third parties, not limiting the obligations to just organisations that outsource work to third parties.

Principle 7: Security

Principle: A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

Rationale: The security principle ensures that data controllers put in place the necessary technical, administrative, and physical safeguards for protecting personal information in their custody from unauthorised use, destruction, modification, access, and retention etc. – both from insiders and outsiders.

Issues and Developments: Security is treated as a cost-centre in organisations, hence the approach to security remains reactive and compliance driven.

- Organisations do not have the central visibility over how the personal information is collected, processed, transferred, disposed, etc. across different units, functions, processes, etc.; this results in lack of organisational control over personal information, leaving many lacunae in the protection of personal information.
- Organisational security efforts are not data-centric but more process focused; they are thus not aligned to the threat landscape that exists currently.
- Managing insider threats is also becoming a big challenge.

Given the above challenges, organisations need to focus on bringing dynamism in security to address real threats in its environment, without focusing only on compliance with regulations. Organisations need to assess their maturity in implementing security in different areas with a view to continually improve the same. Based on this, organisations should draw a strategic plan based on evolution of different disciplines of security, and their interdependencies, with continuous focus on protecting data by adopting a **data-centric methodology.**

Principle 8: Openness

Principle: A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

Rationale: The openness principle ensures that data controllers make their privacy policies, practices, systems, and related developments open, transparent, and accessible to individuals through mechanisms such as providing information in multiple languages, and adopting an open standards/accessible format for the disabled.

Issues and Developments: Organisations do not disclose full information about their information practices on an ongoing basis or make statements that are too generic / vague / complex to reflect their commitment to privacy protection.

Principle 9: Accountability

Principle: The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

Rationale: The accountability principle ensures that the data controller or overseeing body is accountable to the individual, privacy commissioner, and other stakeholders for compliance with all National Privacy Principles.

Issues and Developments:
Accountability is emerging as the foundational principle in privacy. Accountability, although a distinct privacy principle, subsumes the intent of most of the privacy principles and provides directions for enterprise wide implementation of privacy. For the commitment to accountability, organisations are expected to undertake a trust building exercise in respect of its responsibility towards privacy.

Its implementation, however, can be made effective only through regulations that focus on outcome and leave the specifics of implementation to the organisations, which can develop their own programs and structures that are aligned to the respective environments in which they operate, for achieving the outcomes. This approach overcomes the 'one size fits all' problem. Complementing this approach is the concept of self-regulation which helps make the privacy and security programs of organisations relevant and contemporary, as policies and regulations fail to keep pace with technological developments. However, in case of any breach / incident, the onus to prove due diligence lies with the organisations and hence compliance demonstration becomes very important in the implementation of accountability.

Three distinct privacy regulations namely HIPAA, Massachusetts Standards for the Protection of Personal Information and GLBA rely on accountability for privacy regulation. They specify requirements such as policy requirements, executive oversight, risk assessment, policy program, internal enforcement, etc. However, the extent and granularity of regulatory measures have been a major topic of discussion. In the case of Massachusetts, the regulation stipulated a granular level of controls like encrypting the hard disk. Such a granular regulatory approach may lead to multiple problems, as that will be taken as a baseline for implementation, irrespective of the actual security and privacy risks faced. It may also bring rigidity in the control implementation, as the regulations may not able to keep apace with technology and business trend.

Accountability also subsumes the following new concepts:

- Privacy by Design which requires organisations to incorporate privacy requirements in the design of products and services
- Privacy Enhancing Technologies that allow individuals to withhold their true identity from those who operate systems or provide services through them and only reveal it when absolutely necessary.

Currently, privacy protection in India is piecemeal and does not uphold these principles in a systematic function as demonstrated in chapter 4. Thus, an overarching Privacy Act which specifically incorporates these principles and sets up an enforcement mechanism to ensure compliance is an immediate necessity.

Chapter 4: Analysis of Relevant Legislations/ Bills/Interests from a Privacy Perspective

4.1. Several existing legislations in India as well as many proposed ones have grave privacy implications that are scarcely recognised. This chapter discusses some the key legislations in this context, how they conflict with the right to privacy and the provisions which need to be added in order to ensure their overall coherence within the scheme of the proposed privacy regime.

4.2. **The Right to Information:** In many countries citizens are able to hold governments transparent and accountable through Freedom of Information laws, Access to Information laws, and Public Information laws. In India, the Right to Information Act works to promote transparency, contain corruption, and hold the Government accountable to the people. The RTI establishes a responsibility on public bodies to disclose pre-identified information, the right of citizens to request information held by public authorities from public information officers, and creates a Central Information Commissioner responsible for hearing/investigating individual complaints when information is denied.[lx] . In the context of the RTI Act, every public authority must provide information relating to workings of public authorities as listed under section 4 (1(b)) to the public on a suo motu basis at regular intervals. Section 8 of the Act lists specific types of information that are exempted from public disclosure in order to protect privacy. In this way privacy is the narrow exception to the right to information. When contested, the Information Commissioners will use a public interest test to determine whether the individual's right to privacy should be trumped by the public's right to information. There exist more than 400 cases where the Central Information Commissioner has pronounced on the balance between privacy and transparency.

4.3. When applied, the Privacy Act should not circumscribe the Right to Information Act. Additionally, RTI recipients should not be considered a data controller.

4.4. **Freedom of Expression**: The freedom of expression is guaranteed under Article 19(1) (a) of the Indian Constitution. Restrictions on the exercise of the freedom of expression are found in Article 19(2) and can be invoked by the State in the interests of sovereignty and integrity of the State, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offense. When considering the freedom of expression and privacy, there is a fundamental question about the relative weight of privacy and expression. Because the two values are in tension a decision to protect privacy could limit free expression, and a decision to protect free expression could limit the right to privacy, and public interest is used as the test to determine the right balance. Examples of instances in which the freedom of expression needs to be negotiated with the right to privacy include:

4.5. **Public Figures:** To what extent should the freedom of expression be limited in order to protect the privacy of public figures? In India, what aspects of a public figure's life should remain private has been in part defined by the Right to Information Act, but has not been defined for public figures who are not government employees.

4.6. There are also requirements of public disclosures of information relating to public figures that are imposed by various laws and public authorities in the public interest. Examples of this include requirements by the Election Commission of India of all

candidates for elections disclose their private assets, declaration of assets by judges and by other public officials.

4.7. **The Right to be Forgotten and Data Portability:** Should an individual have the right to request deletion of information that pertains to them that has already been circulated on the Internet?

4.8. **Journalistic expression:** Under what circumstances and to what type of data would coverage by a journalist amount to an invasion of privacy of the individual, and when should the privacy right of the ordinary citizen, particularly children, women, minorities, disabled etc be protected against the public's right to be informed.

4.9. **State Secrecy and whistle blowers:** During a sting operation or act of whistle blowing information about public figures, elites, ordinary persons may also enter the public domain. Therefore a public interest test is necessary to determine whether personal information should have been disclosed along with all the other material gathered during the sting operation/whistle blowing.

4.10. **National Security**: To what extent should the privacy of individuals be invaded and limited to protect national security. For example, how this balance should be incorporated into legislation like the Information Technology Act, the National Security Act, and the National Investigation Agency Act.

4.11. Examples of Sectoral Legislation and Policy with Privacy Implications

Banking

1. The Negotiable Instruments Act, 1881
2. The Prevention of Money Laundering Act, 2002
3. The Bankers Book Evidence Act, 1891
4. Credit Information Companies (Regulation) Act, 2005
5. The Insurance Act, 1999
6. Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983
7. Payment and Settlement Systems Act, 2007
8. The Banking Regulation Act, 1949
9. Indian Income Tax Act, 1961
10. Foreign Contribution Regulation Act, 2010
11. RBI Guidelines
12. Fair Practice Code for Credit Card Operations, 2010
13. Gopalkrishna Working Group report, 2011

E-governance & Identity

1. The Passport Act, 1967
2. The Representation of People Act, 1950
3. The Indian Penal Code, 1860
4. The Census Act, 1948
5. The Citizenship Act, 1955
6. The Registration of Births and Deaths Act, 1969
7. The Collection of Statistics Act, 2008
8. The Unique Identification Bill, 2010
9. The DNA Profiling Bill, 2007

Consumer

1. The Contract Act, 1872

2. The Indian Consumer Act, 1986

Freedom of Expression

1. The Press Council Act, 1978
2. Cable Television Networks Regulations Act, 1995
3. Content Certification Rules, 2008
4. Justice (Care and Protection of Children) Act, 2000
5. Contempt of Courts Act, 1971
6. Code of Criminal Procedure, 1973
7. The Indian Copyright Act, 1957

Law Enforcement

1. The National Security Act, 1980
2. The Indian Evidence Act, 1872
3. National Investigation Agency Act, 2008
4. Intelligences Organizations (Restrictions of Rights) Act, 1985
5. Central Bureaus of Investigations Bill, 2010
6. The Intelligence Services (Powers and Regulations) Bill, 2011

Internet and Communications

6.1. The Information Technology Act 2000
6.2. The Telegraph Act 1885
6.3. The Unlawful Activities (Prevention) Act, 2002
6.4. ISP License
6.5. UASL License
6.6. TRAI Regulations on Unsolicited Marketing Calls

Medical

1. Medical Council of India's Code of Ethics Regulations, 2002
2. Epidemic Diseases Act, 1897
3. Mental Health Act, 1987
4. The Persons with Disabilities Act, 1955
5. Pre-Natal Diagnostic Techniques Act, 1994
6. Medical Termination of Pregnancy Act, 1971
7. Ethical Guidelines for Biomedical Research on Human Subjects

Transparency

1. The Right to Information Act, 2005
2. The Official Secrets Act, 1923
3. The Prevention of Corruption Act, 1988
4. The Securities and Exchange Board of India Act, 1992
5. The Monopolies and Restrictive Trade Practices Act, 1969
6. The LokPal Bill, 2011
7. The Public Interest Disclosure and Protection to Persons Making Disclosures Bill, 2010

Application of National Privacy Principles to Existing and Proposed Legislations Human DNA Profiling (HDP) Draft Bill[lxi]

4.12. In 2012 the Draft DNA Profiling Bill was piloted by the Department of Biotechnology, Ministry of Science and Technology, Government of India. The DNA Profiling Bill intends to legalize the collection and analysis of DNA samples of offenders, suspects, missing persons, unknown deceased persons, and 'volunteers' for forensic purposes. This list may be expanded by regulations made under this law. The Bill provides for the creation of a centralized national database of DNA profiles, setting up of a DNA Profiling Board, and sharing of criminals' DNA profiles with other countries to tackle terrorism. It includes provisions to establish standards for laboratories, staff qualifications, collection of body substances, policies of use and access for DNA samples, and the retention and deletion of DNA samples. .

1. Notice

Missing Provisions

- **Notice of collection:** The Bill should require that either after DNA has been collected [but before it is analyzed] or before DNA is collected, the individual is provided with notice that DNA samples or other personal information were collected, the purpose for which they were collected, the use of the collected material, the persons or organizations to whom personal information may be disclosed, the security safeguards established by the organization in relation to the personal information, the processes available to data subjects to access and correct their own personal information, and the contact details of the privacy officers and SRO ombudsmen for filing complaints information and notice to be provided to individuals after DNA is taken.
- **Privacy Notice**: Anybody or organization that collects DNA should be required to provide a public privacy notice.
- **Notice of breach**: The Bill should provide that if a breach occurs or there is a possibility that a sample was contaminated, affected individuals must be given notice.
- **Notice of legal access**: If a DNA profile is legally accessed, the affected individual should be given notice after the investigation is closed.
- **Notice of change in privacy policy**: If there is a change in a collecting or processing organizations practices regarding the collection, storing, processing, use, retention, disclosure, and deletion of information – notice of these changes must be made public.

2. Choice and Consent

Missing Provisions:

- **Circumstances for consent**: Circumstances where the collection of DNA must be done with consent (from a victim or for elimination purposes) and circumstances where collection can take place without consent (crime scene samples) should be distinguished.

Conflicting Provisions:

- **Volunteers*:*** The DNA Data Bank has additionally been entitled to hold indices of volunteers. However, no procedure for requirement of consent, etc. has been provided, and no mechanism has been provided for volunteers to withdraw their information if they desire. ***Section 32***

3. Collection Limitation

Existing Provisions:

- **Prior Approval:** No DNA laboratory will undertake human DNA procedures without obtaining approval in writing from the Board. ***Section 13***
- **Specified Information for Indices**: Every DNA Data Bank shall maintain indices pertaining to crime scene, suspects, offenders, missing persons, unknown deceased persons, volunteers and such other indices as specified under regulations made by the Board. The offenders' index is to contain information relating to the identity of the person from whose body substance or substances the DNA sample was derived, and in case of all other profiles, the case reference number of the investigation associated with the body substance or substances from which the profile was derived. ***Section 32***

Missing Provisions:

- **Notice of Collection**: The Act should specify that only DNA samples and additional personal information specified under the Act can be collected, after when applicable notice has been given, and consent taken.
- **Collection by law enforcement and medical professionals**: Any collection by law enforcement must be done in accordance with laws in force. Circumstances of when medical professionals can collect DNA samples should be specified.
- **Necessary**: Only information relevant and necessary for the stated purpose should be collected.

Conflicting Provisions:

- **Vague Definitions***:* A number of the Bill's definitions are vague, thus further expanding the scope for permitted collection. For example: The "*crime scene index*" is defined to include *"DNA profiles from forensic material found ...on or within the body of any person, on anything, or at any place, associated with the commission of a specified offence."* A *"specified offence"* is defined as *"any of a number of more serious crimes, "or any other offence specified in the Schedule.*" The "*Schedule*," lists various crimes from rape, to "*offences relating to dowry,*" *defamation, and "unnatural offences.*" The term "*suspect*" is defined as anyone *"suspected of having committed an offence.*" ***Section2***

4. Purpose Limitation

Existing Provisions

- **Establishment of databanks**: The Central Government shall establish a National DNA Data Bank and many Regional DNA Data Banks. Every state government may establish a state DNA databank which will share information the National DNA Data Bank. ***Section 32***
- **Use of DNA Profiles and Samples:** DNA profiles and samples can be used only for the purpose of facilitating the identification of offenders with respect to offenders

listed in the Schedule to the Act, and to identify victims, missing persons etc. related to civil disputes, civil matters listed in the Schedule. ***Section 39***

- **Data Retention:** The information in the offenders' index shall be kept on a permanent basis, unless the individual is acquitted, in which case it will be destroyed. ***Section 37***
- **Deletion of information**: The DNA profile of a person will be expunged from the offender's index if he has been acquitted of the charge against him or his conviction has been set aside by the court. ***Section 37(2)***
- **Use Limitation:** DNA profiles for entry into the DNA Data Bank shall only be used for purposes specified under the Act. **Section 44(1)** No person to whom information is communicated shall use that information for any other purpose. ***Section 44(3)***

Missing Provisions

- **Adequate and Relevant:** All collection and processing of DNA samples and personal information must be adequate for the purposes specified in the Act. The purpose must be clear and specific, and the law may extend to meet the stated purpose.
- **Notice of purpose:** Where applicable, notice of the purposes for collection of DNA samples and personal information must be made public.
- **Use Limitation**: All use of DNA samples and personal information should be limited to the purposes and timeframe specified by the Act. For example, DNA samples collected for forensic purposes should be restricted from being used for other purposes like health research, or behavioral research.
- **Retention Period**: A retention period that is in compliance with the National Privacy Principles should be established. For example, this should include clear instructions for segregation / separation of the indices – crime scene, suspects', offenders', missing persons', unknown deceased persons' and a volunteers' in the Data Banks. DNA evidence collected should be retained only as long as is necessary to achieve the objective of the collection.
- **Destruction Procedure:** A procedure for the destruction of all DNA samples and collected personal information after it has served its purpose should be established. For example, DNA samples should be destroyed once the DNA profiles needed for identification purposes have been obtained from the individual. Data stored on DNA databases pertaining to innocent persons should be automatically removed and deleted from the database. Linked data on other databases (police records of arrest, fingerprints) should be deleted at the same time as DNA database records.

Conflicting Provisions

- **Expansion of Use and Purpose**: The DNA Board is responsible for making "recommendations for maximizing the use of DNA techniques and technologies in administration of justice". The DNA Board is also responsible for specifying in regulations the collection, use, security, confidentiality etc. of DNA information. This could serve to take the use of DNA samples and the purpose of the Bill beyond the administration of justice. ***Section 12***
- **Broad Storage of Indices**: Every DNA data bank must maintain indices for: crime scenes, suspects, offenders, missing persons, unknown deceased persons, volunteers, other indices that might be specified by the Board. ***Section 32(4)*** The indices must include information of DNA identification records and DNA analysis. ***Section 32(5)*** In the case of the offender's index, the identity of the person, and in the case of all

other profiles, the case reference number of the investigation with the body substance from which the profile was derived. ***Section 32(6)***

- **Use of previously collected information:** All DNA laboratories in existence at the time the legislation is enacted are allowed to process or analyze DNA samples immediately, without first obtaining approval. ***Section 14 – 15***
- **Broad use of genetic material**: The national database is envisioned to comprise of several sub-databases, each to contain the genetic information of a subset of persons/samples, namely: (1) unidentified crime scene samples, (2) samples taken from suspects, (3) samples taken from persons convicted or currently subject to prosecution for "subject offences," (4) samples associated with missing persons, (5) samples taken from unidentified bodies, (6) samples taken from "volunteers," and finally (7) samples taken for reasons "as may be specified by regulations." ***Section 33(4).***
- **Broad Access**: DNA profiles, DNA samples, and information relating thereof can be made available for identification purposes in a criminal case to law enforcement agencies, in judicial proceedings, for facilitating decisions in cases of criminal prosecution, for defense purposes to the accused, for creation and maintenance of a population statistics database provided it does not contain personally identifiable information, and in the case of investigations related to civil disputes. ***Section 40*** Any person authorized to access the DNA Data Bank for the purpose of including DNA information that has been legally obtained, by also complete a one-time keyboard search on information obtained, except if the sample is voluntarily submitted. ***Section 42*** Access to DNA profiles is restricted only for victims and persons who have been excluded as a suspect. ***Section 43***

5. Access and Correction

Missing Provisions

- **Right to correct:** Individual's should have the right to view and correct personal data contained on a DNA database.
- **Right to Access:** Individual's should have the right to request if a lab or DNA processing organization holds any personal information pertaining to them.
- **Limited Access:** Access to personal information on request should be limited until consent is obtained if another's personal information will also be disclosed.

6. Disclosure of Information

Existing Provisions

- **Instances for disclosure**: The Act enlists instances in which information relating to DNA profiles, DNA samples, and records should be made available. Furthermore, the Board has been granted the right to make DNA information available for such other purposes as it may prescribe. ***Section 40***

Missing Provisions

- **Compliance with the National Privacy Principles**: The Act should require that all third parties must be bound by the National Privacy Principles.
- **Notice and consent for Disclosure:** The Act should require that notice must be provided to the individual if their information is disclosed to a third party, and consent taken, unless the disclosure is required by authorized agencies.

- **Law Enforcement:** Disclosure to law enforcement for purposes under Article 19(2) must be done in accordance with laws in force.

7. Security

Existing Provisions

- **Quality of DNA laboratories:** Every DNA laboratory that has been granted approval by the board is required to follow specified regulations, establish and maintain a documented quality system, establish and maintain quality manual details. ***Section 18***
- **Confidentiality:** The confidentiality of DNA profiles and DNA samples and records in custody of the DNA Data Bank Manager or DNA laboratory or any other person or authority under the Act must be maintained. ***Section 38***
- **Security and Integrity of Samples:** DNA laboratories are required to ensure the integrity and security of the DNA information and samples. ***Section 21*** This includes having a documented evidence control system in place to ensure the integrity of physical evidence ***Section 22,*** having a validation process in place ***section 23,*** using suitable equipment for the methods employed. ***Section 26***
- **Security of Personnel:** Every laboratory shall have installed security systems for the safety of personnel. ***Section 31***

Conflicting Provisions

- **Communication to Foreign States**: - Communication of any DNA profiles to foreign states, agencies, international organisations etc. is not restricted to the offenders' index alone, thus allowing for the DNA profiles of missing persons, volunteers, and victims to be communicated. ***Section 36***
- **Broad Communication:** When the Data Bank Manager considers it to be appropriate, he may communicate to a court, law enforcement agency, or DNA laboratory whether a DNA profile is already in the Data Bank, if any other information other than a DNA profile is in the Data Bank, whether a person's DNA profile is contained in the offender's index**.** ***Section 35***

8. Openness

Missing Provisions

- **Transparency Report**: Bodies and organizations collecting, analyzing, and storing DNA samples should publish a transparency report on an annual basis detailing their internal governance structure, practices, finances, and success and error rates. This should include the DNA profiling board.

9. Accountability

Existing Provisions

- **The DNA Profiling Board**: The DNA Profiling Board is given the power to make recommendations for provision of privacy protection laws, regulations and practices regarding DNA analysis and access to or use of stored DNA samples. The Board is also responsible for making recommendations to ensure the appropriate use and dissemination of DNA information, ensure the security and confidentiality of DNA information, and ensure the timely removal and destruction of obsolete or inaccurate information. ***Section 12***

- **The DNA Data Bank Manager**: The DNA Data Bank Manager has the sole right to supervise the actions of the DNA Data Bank, and to access all DNA information therein. The DNA Data Bank Manager is empowered to grant the right to such other persons or class of persons as it desires, for the purpose of proper operation and maintenance of the DNA Data Bank, as well as for training. ***Section 41***
- **Offences and Penalties**: The HDP Bill has made provisions for offences in relation to the unauthorized disclosure, usage, destruction, transfer, access etc. to DNA information, profiles and samples. It has also addressed offences committed by companies and institutions under its purview. ***Section 52 – 58***
- **Cancellation of Approval:** The Board may withdraw granted approval to DNA laboratories if the laboratory fails to comply with required conditions by the board, by in law in force, or fails to submit for inspection books, accounts, and relevant documents. **Section 16**
- **Audits**: Every DNA laboratory must conduct audits annually in accordance with specified standards. ***Section 27***

Missing Provisions

- **Redress and compensation**: The Bill should create a redressal mechanism for individuals whose DNA was illegally used or collected, or against offences committed by the Board itself. As part of this, individuals should be given a private cause of action for the unlawful collection of DNA, and for the unlawful storage of private information on the national DNA database. A process of appeals against the retention of data should also be made available to individuals, and individuals should be able to have a second sample taken and reanalyzed in court.

Conflicting Provisions

- **Complaints**: Only the Central Government or DNA Profiling Board is empowered to bring complaints to the courts. ***Section 58***

10. Verification

Missing Provisions: There is no process in place to verify the correctness of the DNA analysis and the information placed in the DNA databases.

Citizenship Act, 1955 and Rules, 2003[lxii]

4.13. Section 14A of the Citizenship Act empowers the central government to compulsorily register every citizen of India and to issue national identity cards to every citizen. It also empowers the government to establish and maintain a National Register of Indian Citizens, and authorizes the Registrar General of India to act as the National Registration Authority for this purpose. The Citizenship Rules, 2003 detail the information that will be maintained in the national register for every citizen. According to the Act, the National Register will be divided into four sub-parts: state register, district register, sub-district register and the local register.

1. Notice

Existing provisions

- **Notice of Collection:** The Registrar General will notify the period and the duration of the enumeration in the Official Gazette. ***Rule 4(2)***
- **Notice of Removal:** The citizen will be duly informed if his information is removed from the national register for legitimate reasons such revocation of citizenship, incorrect information provided, death (nearest relative to be informed), etc. ***Rule 10 (3)***
- **Notice of Verification:** If an individual's particulars have been scrutinized for verification, once the verification is completed, the individual will be informed immediately. ***Rule 4(4)***
- **Notice of Initialization:** The Registrar General of Citizen Registration will notify the date on which the National Register of Indian Citizens will be initialized. ***Rule 6***

Missing provisions

- **Notice During Collection**: During collection information the individual should be notified by the collecting official that: personal information is being collected, the purposes for which the personal information is being collected, the uses of the collected personal information, the persons or organizations to whom personal information may be disclosed, the security safeguards established by the organization in relation to the personal information, the processes available to data subjects to access and correct their own personal information, the contact details of the privacy officers and SRO ombudsmen for filing complaints.
- **Notice of Data breach:** If a data breach occurs, affected individuals are informed.
- **Notice of legal access**: If any personal information is legally accessed, individuals should be notified after the closure of the investigation.
- **Notice of change in privacy policy**: If the government changes its practices regarding the collection, storing, processing, use, retention, disclosure, and deletion of information – notice of these changes must be made public.
- **Notice of modification**: The Act should require notification to the individual when their information is legally modified by the Register General or authorized officers.

2. Choice and Consent

Existing Provisions

- **Mandatory Registration:** Every individual must register with the Local Register of Citizen Registration during the period of initialization. ***Rule 6(3)*** It will be the responsibility of the head of every family to give correct details of name and number of members and other particulars as specified. ***Rule 7(2)***

Missing Provisions

- **Mandatory provision in compliance with National Privacy Principles:** Where mandatory provision or collection of information is required, this must be done in compliance with the National Privacy Principles.

3. Collection Limitation

Existing Provisions

- **Authority to determine information fields**: The Registrar General is empowered to determine what information should be included in the National Register of Indian Citizens. ***Rule 3(2)***
- **Information fields**: The following will be collected - Name, Father's Name, Mother's Name, Sex, Date of Birth, Place of Birth, Residential Address (present and permanent), Marital Status [if ever married, name of spouse], Visible Identification Mark, Date of registration of Citizen, Serial no. of registration, National Identity Number. ***Rule 3(3)***
- **Collection Methods:** House to house enumeration will be carried out for the collection of specified particulars. ***Rule 4***

Conflicting Provisions

- **Power to require information:** The Act provides the district registrar, sub-district or taluk register, or local register of Citizen Registration the power to require any person to furnish any information within his knowledge in connection with the determination of Citizenship status of any person and binds the person to comply. ***Rule 8***
- **Fields of information**: The purpose of collecting information on marital status, and the usefulness of visible identification marks across the whole population may need to be revisited.

4. Purpose Limitation

Existing Provisions

- **Deletion Policy**: The name and particulars of a Citizen may be removed from the National Register of Indian Citizens by an order of the Register General of Citizen Registration in the event of death, ceasing of Indian Citizenship, revocation of Indian Citizenship, incorrect particulars. ***Rule 10(1)***
- **National Identity Cards**: The Registrar General of Citizen Registration will issue a National Identity Card to every Citizen whose particulars are entered in the National Register of Indian Citizens. ***Rule 13***

Missing Provisions

- **Use Limitation:** The Act should specify that personal information can only be collected, disclosed, made available, accessed, or otherwise used personal for the purposes and time frame specified by the Act, and as provided in the notice to the individual. Where applicable, consent should be taken from the individual.
- **Law Enforcement**: The Act should establish a clear procedure for access to information by law enforcement that is in compliance with laws in force.
- **Use of National Identity Card:** The Act should clarify the permitted and prohibiteduses of the National Identity card.

5. Access and Correction

Existing Provisions

- **Right to correction:** The citizen can make an application to the concerned authority for modifying his information [name, name of parents, residential address, marital status, sex] stored in the national register. Such modifications can be allowed only after due verification of the changes requested. ***Rule 12***

Missing Provisions

- **Right to Access:** Citizens should have the right to confirm and access any personal information held by the RGI.
- **Right to Access Disclosures:** Citizens should have the right to request to whom their personal data has been disclosed.
- **Access/disclosure not to impact others:** The Act should specify that if any request for access and disclosure requires that information pertaining to another person is disclosed, the access/disclosure will not be allowed without consent.

6. Disclosure of Information

Missing Provisions

- **Subcontracted agencies:** The Act should require notice to be provided if private agencies will be sub-contracted for the collection and processing of information, and maintenance of the national register. All third parties should be bound to adhere to the National Privacy Principles.
- **Information available from ID cards**: The Act should clarify what information will be accessible to third parties when an individual uses his/her card.

7. Security

Missing Provisions

- **Security measure:** The Act should specify security and privacy measures that will be taken by the government to protect data collected and stored against loss, unauthorized access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental], or other reasonably foreseeable risks.

8. Openness

Missing Provisions

- **Transparency**: The Government should make open to the public in an intelligible form, using clear and plain language information concerning the steps they have taken to comply with the National Privacy Principles.

9. Accountability

Existing Provisions

- **Assistance in enforcement:** Officials of the Central Government, State Governments and local bodies must assist the Registrar General of Citizen Registration in implementing the provisions of the Act and Rules. ***Rule 5***
- **Appeal:** Every individual will be given the opportunity to be heard by the sub-district or Taluk Registrar before a final decision is taken to include or exclude their

particulars in the National Register of Indian Citizens. ***Rule 4(5)*** Any person aggrieved by the order of the sub-district or Taluk Register may appeal to the District Registrar of Citizen Registration within thirty days. ***Rule 7(a)*** Any person aggrieved by the order of any authorized officer may take the appeal to the Authority within a period of thirty days. ***Rule 10(3)***

- **Penalty:** Any violation of provisions 5, 7, 8, 10, 11, and 14 will be punishable with a fine which will extend to rs. 1,000. ***Rule 17***

Missing Provisions:

- **Rights of appeal:** The Act should give individuals the right to appeal orders of the RGI in a court. Currently, the rules allow individuals to take appeals only to the Authority (Registrars).
- **Sufficient Penalties:** The violation of provisions of the rules is punishable with fine which may extend to one thousand rupees. Breaches of privacy have not been considered while making this rule.

Conflicting Provisions:

- **Disposals of Appeals:** The Registrar General may specify the procedure to be followed in preparation of the National Register and disposal of claims and objections with regards to family and individual particular proposed to be entered into the Register. ***Rule 9***

10. Verification

Existing Provisions

- **Inclusion and exclusion of information:** The Registrar General of India (RGI) or any officer authorized by him has been empowered to issue directions regarding inclusion or exclusion of any individual or family particulars from the national register. ***Rule 16(5)***
- **Inclusion after verification**: The Local Register of Indian Citizens will contain details of persons only after due verification made from the Population Register. ***Rule 3(5)*** These particulars will be verified and scrutinized by the Local Registrar. ***Rule 4(3)*** During the verification process, particulars of those individuals whose Citizenship is doubtful, will be entered into the Local Register with remark for further enquiry. ***Rule 4(4)***
- **Public verification of information:** For data quality purposes, the draft local register containing the collected personal details of the citizens will be published for inviting any objections or for inclusion of any name or corrections before this information is entered in the National Register of Indian Citizens**.** Within a period of ninety days, the Sub district or Taluk Register will consider such objections and summarily dispose of the same. Post verification the data from the local register will be entered in the national register. ***Rule 4(6 a-c)***
- **Maintenance and Updating:** The Registrar General of Citizen Registration will be responsible for maintaining the National Register of Indian Citizens in electronic format, which will entail its continuous updating on the basis of extracts from Registers found under the Registration of Births and Deaths Act. The Chief Registrar of Births and Deaths and all other officials engaged in the registration of births and deaths will assist the Registrar General of Citizen Registration in updating the National Register of Indian Citizens. ***Rule 11***

Collection of Statistics Act, 2008 and Collection of Statistics Rules, 2011[lxiii]

4.14. The Collection of Statistics Act, 2008 was brought into force in 2010. The Collection of Statistics Rules were notified in 2011. The Collection of Statistics Act and the Rules provide for the collection of statistics on economic, demographic, social, scientific and environmental aspects from industrial and commercial organizations, individuals, and households.

1. **Notice**

Existing Provisions

- **Notice of disclosure:** The appropriate government or a statistics officer must indicate in each information schedule its plan, if any, to disclose any information collected from them which in the opinion of the appropriate government is available to the public under any other Act or as a public document or which is in the form of an index or list of the names and addresses of informants together with the classification allotted to them and the number of persons engaged. ***Rule 6(x)***
- **Notice of receiving information:** The statistics officer will cause notice to informants for furnishing information issued under his signature, and where necessary cause acknowledgments received from such informants, to be kept in safe custody. ***Rule 9(ix)***
- **Notice of statistics officer:** Every notification appointing a statistics officer should contain the name, designation, and address of the officer, the details of the any agency, company, organization, association, or person engaged for collection statistics and terms and conditions of engagement and safeguards laid down for the purpose, the form and the particulars required or the interval within which, and the statistics officer to whom, the statistical information by the informants will be furnished, and the powers delegated to any statistics officer. ***Rule 7***

Missing Provisions

- **Notice during collection**: During collection of statistics an officer should be required to provide notice that: personal information is being collected, the purposes for that collected information, and the uses of the collected personal information, the organizations to whom personal information might be disclosed, the security safeguards in place, the process for individuals to access and correct their information, and the contact details of the officer to issue complaints.
- **Notice of legal access or data breach**: Notice should be given to the individual if any personal information is legally accessed. If a data breach occurs either when information is held by a statistical officer or when it is held by a subcontracted body, affected individuals should be notified immediately.

2. **Choice and Consent**

Existing Provisions

- **Discretion of the informant**: Each information schedule used for collecting statistics from any informant must have, where necessary, a provision for particulars on which information may be furnished at the discretion of the informant. ***Rule 6(viii)***
- **Consent for disclosure:** The appropriate government or a statistics officer must make provision in each information schedule to obtain written consent

from each informant when collecting information that it proposes to disclose. ***Rule 6(xi)***

Missing Provisions

- **Mandated provision in compliance with Privacy Principles**: The mandatory legal requirement that informants provide requested information found under the Act should be in compliance with the National Privacy Principles. All information collected on a mandatory basis should be anonymized within one year.

Conflicting Provisions

- **Legal obligation to furnish information:** Individuals are required to furnish all requested information. The obligation to furnish information under the Act will not cease after conviction for an offence. If the concerned person continues to neglect or refuse to furnish information after the expiry of fourteen days from the date of conviction, then he may be punished with a further fine up to Rs.1,000/- (Rs.5,000/- in case of a company) for each day after the first during which the failure continues. ***Section 15(2)***

3. Collection Limitation

Existing Provisions

- **Collecting Authorities and Agencies:** The appropriate Government may appoint a statistics officer for any geographical unit for the purpose of collecting statistics. The appropriate Government may also appoint any agency to aid or supervise the collection of statistics. The Government may employ on a contract basis any agency for the purpose of collecting statistics. The appropriate Government may delegate any statistics officer for the purpose of collection of statistics. ***Section 4(1-6)***
- **Collection Limitation:** The appropriate government or a statistics officer shall satisfy itself that the range and detail in the information schedules specified for collection of statistics on any subject shall be limited to what is absolutely necessary ***Rule 6(iv)***
- **Collection Methods**: The methods of oral interviews, filing of returns electronically, fax, telephone, and email are to be employed for data collection. ***Section 5***
- **Format for furnishing Information**: The appropriate Government may specify the form, the particulars required, the intervals within which, and the statistics officer to whom informants should furnish statistical information. ***Section 4(4)***

Missing Provisions

- **Notification of purposes for collection**: Persons authorized by the Act should only collect personal information for specific purposes [beyond 'statistical purposes] that have been notified to the public and in the Act.

Conflicting Provisions

- **Broad mandatory collection:** The statistics officer may serve any informant a notice in writing asking him to furnish information specified by the Act, cause questions relating to the subject to be asked from any informant, seek information through telefax telephone, email, or any other electronic mode. ***Section 5***
- **Agencies to Furnish Information:** Every agency shall furnish information to the statistics officer and shall make available for inspection and examination records, plans, and other documents as may be necessary. ***Section 7***

- **Access to Records:** The statistics officer for the purpose of collection of any statistics have access to any relevant record or document in the possession of any informant. The officer may enter at any reasonable time any premise where he believes the record might be kept, and may inspect, take copies, or ask questions for obtaining needed information. ***Section 8***

4. Purpose Limitation

Existing Provisions

- **Purpose:** The appropriate Government will direct that the statistics on economic, demographic, social, scientific, and environmental aspect shall be collected through a statistical survey. ***Section 3***
- **Use limitation**: The information collected from any informant under the Act cannot be made use of for any purpose other than for prosecution under the Act or for statistical purposes. ***Section9(1)***
- **Access limitation:** No person other than that engaged in the work of the collection of statistics shall be permitted to see any information schedule or any answer to question asked**.** ***Section 9(2)***
- **Anonymization:** No information or answer to any question shall be separately published or disclosed without suppressing the identification of informants to any agency. ***Section 9(3)***
- **Principles for Information schedules:** When prescribing any information schedule for the collection of statistics, the government or statistics officer must be satisfied that it has the authority to direct collection, it has consulted the nodal officer, excessive demands are not placed on the informants, the details required are limited to what is necessary, the reporting burden is spread widely, the information sought from business is as far as possible, readily available from their accounts and electronic means should be used where possible to collect, best estimates where exact details are not available, individuals are given the option to provide certain categories of information, each information schedule indicates its place, if any to disclose information, make provisions to obtain written consent when non-required information is proposed to be disclosed**.** ***Rule 6***
- **Outsourced agencies:** Any agency subcontracted out to may only use personal formation for the purpose of fulfilling its obligations specified under contract. ***Rule 13***

Missing Provisions

- **Adequate and Relevant:** Personal data collected must be adequate and relevant for the purposes of compiling statistics.
- **Data retention mandates**: All data retention mandates must be in compliance with the National Privacy Principles.
- **Destruction of information**: After collected information has been used for purposes required under the Act, or has been anonymized, the original information should be destroyed.
- **Notice of change in purpose**: If there is a change of purpose for the collection or use of collected material, this must be notified to the individual.

5. **Access and Correction**

Existing Provisions

- **Access for correction**: Statistical officers must allow access to any informant to the information collected from that informant for facilitating intimation of corrections or amendments on any inaccurate information. ***Rule 9(xiii)***
- **Procedure for access**: The appropriate government or an officer authorized by that government must provide details as to how informants can access their information for making corrections, this includes storing the statistics collected in such a way to allow for easy retrieval of information, and keeping all the undertakings and other material obtained from the statistics officers and other persons or agencies engaged in collection of statistics in safe custody. ***Rule 16***

Missing Provisions:

- **Right to request personal records**: Individuals should have the right to request if a statistical officer has records that contain their personal records, and if so, has the right to request a copy of this information.
- **Right to request information of disclosure**: Individuals should have the right to request to whom their personal information has been disclosed.
- **Access to not violate any other person's privacy**: The Act should specify that access and disclosure cannot be made if it requires the disclosure of another's personal information – until consent has been obtained.

6. **Disclosure of Information**

Existing Provisions

- **Safeguards for subcontracting**: The Act and the Rules prescribe appropriate safeguards when data collection is outsourced including: ***Rule 12&13***
  - Formal and comprehensive contracts that include provisions requiring service providers not to access, use, disclose or retain personal information except in performing their duties of employment or contractual obligations. All personal information may only be used for the purposes specified in the contract.
  - On-site inspections of outsourcing service providers by appropriate government or authorized statistics officers.
  - Applicability of all provisions relating to the disclosure of information and restrictions of its use found under the Act during the duration of the contract and after the termination or completion of the contract.
  - If a statistics officer receives a complaint, they must immediately contact the outsourcing agency in order to minimize any breach.

Missing Provisions

- **Third parties accountable to privacy principles**: All third parties to whom information is disclosed or outsourced to must be held in compliance with the National Privacy Principles by the Act.
- **Notice and consent before disclosure**: The Act should only disclose personal information to third parties after providing notice to the individual and seeking consent, except in the case of disclosure to authorized agencies.
- **Disclosure to law enforcement**: Any disclosure to law enforcement must be in accordance with laws in force and for purposes under Article 19(2).

- **Clear circumstances for disclosure**: The Act and rules must clearly specify the circumstances when information can be released by the government.

Conflicting Provisions

- **Exceptions to Anonymization**: Disclosure of information collected from any person without suppressing the identification particulars of that person is not permitted under the Act except when the disclosure is consented to in writing by the informant, the publication could not have been reasonably foreseen, the information is otherwise considered public, the information is in the form of an index or list of the names and addresses of informants together with the classification and number of persons engaged, is disclosed to any agency, person, institution, or university for research or statistical purposes. ***Section 9, 10, 11***
- **Disclosure for historical purposes**: The appropriate government is allowed to release documents relating to information schedules, which in its opinion, have attained *historical importance*, how this historic attribute will be determined has not been addressed in the Act / rules. ***Section 12***

7. Security

Existing Provisions

- **Security measures**: The statistics officer or any person or agency authorized for collection must take steps to ensure that the security provisions of the Act are complied with. ***Section 13***
- **Agencies to have security measures**: Each agency engaged in collection of statistics shall take reasonable measures to ensure that personal information is protected against unauthorized access, disclosure or other misuse. If an agency is processing data, it must do so only have security checks are in place. ***Rule 13***

Missing Provisions

- **Defined electronic format**: If collected information is converted into electronic format, how this is done, and what type of format should be specified and appropriate security standards put in place.
- **Specific Security measures**: What *specific security and privacy measures* such as privacy impact assessments, audits, prescription of security practices, etc will be taken by the government and partner agencies to protect electronic data should be specified in the Act.

8. Openness

- **Missing Provisions:** An organisation should take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made available to all data subjects in an intelligible form, using clear and plain language.

9. Accountability

Existing Provisions

- **Oversight:** The Central/ State Governments, UT Administrations and the local governments such as Panchayats and Municipalities have been empowered to collect any statistics. Any appropriate government may appoint a statistics officer for each subject of data collection and/ or for each geographical unit.

Section 3 The Central Government will designate an officer not below the rank of a Joint Secretary to the Government of India in a nodal Department dealing with statistical matters. ***Rule 3*** The Nodal Officer will maintain and update register of statistics officers appointed by the Central Government. ***Rule 4***

- **Prevention of Duplication**: The Act empowers the Central Government to make rules for avoiding duplication. The Rules made under the Act provide for designating a nodal officer at the Centre and in each State/ UT to advise the concerned Ministries on steps to be taken to avoid unnecessary duplication. In order to further eliminate de-duplication of information, each appropriate government collecting statistics must record: the subject and purpose for collection of statistics, the geographical area for collection of statistics, the method of data collection, the nature of information from whom data may be collected. The period during which collection of statistics will take place, the nature of the information collected, the language in which the information will be collected, and the obligations of the informant. ***Rule 5(5)***
- **Penalties:** The Act provides for penalties for: furnishing false information, mutilation or defacement of information, failure to carry out duties and functions by persons employed in the execution of any duty including seeking to obtain information which he is not authorized to do and failure to keep secrecy of information gathered, and impersonation of employees. Penalties range from imprisonment up to six months or with a fine or with both. ***Sections 16, 17, 18*** and imprisonment for a term which may extend to 6 months or with a fine which may extend to Rs. 1000/-, or in case of a company, with a fine which may extend to Rs. 5000/. ***Sections 17, 19, 20***
- **Liability**: When an offence is committed by a company, every person shall be deemed guilty under the Act, unless they are able to prove that the offence was committed without his/her knowledge and that he had exercised all due diligence to prevent the commission of the offense. ***Section 23***
- **System of complaints:** If any agency receives any complaint from any informant, it shall immediately communicate the complaint to the appropriate government or the concerned statistics officer. ***Rule 12(i)***

Missing Provisions

- **External Verification:** Mechanisms should be put in place to ensure that external verification takes place on an ongoing basis.
- **Sufficient Fines**: Penalties under the Act should be stringent enough to enforce the provisions.
- **Mechanisms for Redress and Compensation**: Individuals should have the right to initiate proceedings against any offender including the government and seek compensation.

Conflicting Provisions

- **Lack of redress mechanism for individual**: No court shall take cognizance of any offence punishable under the Act, save on a complaint made by the appropriate government or any officer or person authorised by it. ***Section 24***

The National Identification Authority of India Bill, 2010[lxiv]

4.15. The National Identification Authority of India (NIAI) Bill is a proposed legislation meant to provide a legal framework for the National Identification Project, which is envisioned to be an identity scheme meant to issue unique identification/Aadhaar numbers that are based on biometrics to residents on a voluntary basis. The following personal information will be collected for issuance of an Aadhaar number - Name, Date of Birth, Gender, Fathers/Spouse/Guardian's name, Mother/Spouse/Guardians name and Address; Photograph, all ten fingerprints and both iris scan. In addition, information about bank account, introducer, consent, mobile number, email address and the document on which the enrolment is based may be collected.

4.16. The Bill provides for the establishment of a National Identification Authority of India (NIAI) for the purpose of issuing identification or Aadhaar numbers to individuals residing in India, manner of authentication of such individuals, establishment and composition of Authority, functions of Chairperson, and protection of information relating to an Aadhaar number, and penalties for impersonation, unauthorized access, and the power to make rules and regulations in this regard. The NIAI Bill contains detailed provisions on several aspects of the unique identification number and its administration.

1. Notice

Missing Provisions

- **Breach**: Affected individuals should be notified of any breach at the level of enrolling agencies The Bill does not provide for Aadhaar number holders to be notified when their data is accessed or its integrity/security is breached.
- **During Collection**: During enrollment agencies should provide notice of the fact that personal information is being collected, the purposes for which personal information is collected, the uses of collected personal information, the persons or organizations to whom personal information may be disclosed, the security safeguards established by the organization in relation to the personal information, the processes established by the organization in relation to the personal information, the processes available to data subjects to access and correct their own personal information, the contact details of the privacy officers and SRO ombudsmen for filing complaints.
- **Legal Access**: If information is legally accessed, notice should be given to affected individuals after the closure of the investigation.
- **Change in Privacy Policy**: If the privacy policy of any agency collecting information or the UID changes, notice must be given to the public and the individual.

2. Choice and Consent

Existing Provisions

- **Sharing of information:** The UIDAI will create regulations for the sharing of information of Aadhaar number holders with their written consent, with such agencies engaged in the delivery of public benefits and public services. ***Section 23k***

Missing Provisions

- **Opt in or Out:** The Bill should specify that individuals have the choice to opt in or out of providing their Aadhaar number, and a service should not be denied to an individual for not providing their number.

  *******UID however pointed out that the enrolment for* Aadhaar *is upfront voluntary; therefore, it is baseless to say there is no choice available to an individual. As regards access to services it is beyond the remit of this legislation to prescribe across board that without* Aadhaar *a service should not be denied.*
- **Mandated Provision:** The mandatory provision of information to obtain an Aadhaar number should be in compliance with the National Privacy Principles.
- **Anonymization:** If information is collected on a mandatory basis – either by an enrolling agency at the time of enrollment or for the purposes of authentication via the UID, this material should be anonymized within one year if published in public databases.
- **Lack of choice**: Although the Bill states that obtaining the Aadhaar number is not mandatory, it should contain provisions that ensure that enrolment is not made mandatory by any other agencies.

Conflicting Provisions

- **Appropriate Consent**: One of the functions of the Authority under ***Section 23 (2) (k)*** of the Bill is to share the "information of Aadhaar number holders, with their written consent, with such agencies engaged in the delivery of public benefits and public services." Since some Aadhaar applicants may be illiterate, it may not be reasonable for the Authority to expect that the Aadhaar number holders will be able to understand the implications of information sharing and provide their written consent for the same.

3. Collection Limitation

Existing Provisions

- **Limited Collection:** Authority from requiring any individual to give information pertaining to his race, religion, caste, tribe, ethnicity, language, income or health. ***Section 9***

Missing Provisions

- **Proportional**: Enrolling, registering, or otherwise collecting information shall only collect as much information is necessary for the purposes identified by the Bill, and for which notice and consent have been taken.

Conflicting Provisions

- **Transaction Data: The UID** Authority shall maintain details of every request for authentication of the identity of every Aadhaar number holder and the response provided thereon by it in such manner and for such time as may be specified by regulations. ***Section 32***

4. Purpose Limitation

Missing Provisions

- **Adequate and Relevant:** Personal data collected and processed by enrolling agencies and the UIDAI must be adequate and relevant to the purposes for which they are processed.
- **Stated Purposes:** Enrolling agencies, registrars, transacting organizations, and the UIDAI will only collect, disclose, make available, or otherwise use personal

information for the purposes stated in the Bill, as notified to the public, and with consent from individuals.

- **Notification of change in purpose:** If there is a change in purpose, this must be notified to the public and the individual.
- **Destruction:** After personal information has been used in accordance with the identified purpose it must be destroyed as per identified procedure.
- **Data Retention Mandates:** All data retention mandates by enrolling agencies, transacting organizations, and the UIDAI must be in compliance with the National Privacy Principles.

Conflicting Provisions

- **Broad response:** The authority will reply to an authentication request with a yes or no answer, or with any other appropriate response. This introduces the possibility of another response, and may negate the privacy protection of only a yes or no answer, by introducing the possibility for another response. ***Section 5.***
  * *UID's version however is that the authority cannot restrict itself to giving to monosyllabic responses as it may have to take care of communicating through error codes etc.*

5. Disclosure of Information

Missing Provisions

- **Disclosure with consent:** Enrolling agencies, registrars, the UIDAI, and organizations conducting transactions should only disclose information to third parties only if notice has been given and informed consent taken for each transfer.
- **Compliance with National Privacy Principles:** All third parties must be bound to the National Privacy Principles.
- **Disclosure to Law Enforcement:** Disclosures to law enforcement must be made in accordance with laws in force.

Conflicting Provisions

- **Access by law enforcement**: Any collected information can be disclosed pursuant to an order of a competent court; or made in the interests of national security in pursuance of a direction to that effect issued by an officer or officers not below the rank of Joint Secretary or equivalent in the Central Government specifically authorised in this behalf by an order of the Central Government. ***Section 33***
- **Subcontracting/delegation:** The Authority to engage one or more entity for the establishment and maintenance of the CIDR, and for any other function as may be specified. This provision allows for any activity to be delegated and outsourced. ***Section 7***

6. Security

Existing Provisions

- **Security measures:** The Authority shall ensure the security and confidentiality of identity information and authentication records of individuals and take measures (including security safeguards) to ensure that the information in the possession or control of the Authority (including information stored in the Central Identities Data Repository) is secured and protected against any loss or unauthorised access or use or unauthorised disclosure. ***Section 30(1)***
- **Confidentiality:** Notwithstanding anything contained in any other law for the time being in force and save as otherwise provided in the proposed legislation, the Authority or any of its officers or other employee or any agency who maintains

the Central Identities Data Repository shall not reveal any information stored in the Central Identities Data Repository to any person. ***Section 30(2)***

7. **Openness**

Missing Provisions: Enrolling agencies and the UIDAI should make available to all individuals in an intelligible form, using clear and plain language, all steps taken in order to ensure compliance with the privacy principles.

8. **Accountability**

Existing Provisions

- **Authority:** The Bill provides for the establishment of a National Identification Authority of India (NIAI) for the purpose of issuing identification or Aadhaar numbers to individuals residing in India. ***Section 11***
- **Penalties:** Penalties will be issued for impersonation, intentional disclosure to unauthorized individuals, collection of information without authorization for a term which may extend to three years and with a fine which may extend to ten thousand rupees, for unauthorized tampering with the data in the Central Identities Data Repository or in any removable storage medium. ***Section 34***, ***36***, ***37, 39*** for unauthorized access to the Central Identities Data Repository with imprisonment for a term which may extend to three years and shall be liable to a fine which shall not be less than one crore rupees. ***Section 38*** for any other offence under the Act with imprisonment for a term which may extend to three years or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both. ***Clause 41*** The provisions of the legislation will apply to any offence or contravention committed outside India. ***Clause 43***

Missing Provisions

- **Compensation and redress:** The Bill does not provide individuals with clear forms of redress.

Conflicting Provisions

- **Broad Powers**: Among other powers, the Authority has the power to specify required demographic information and biometric information for enrollment and the processes for collection and verification of demographic and biometric information, maintaining and updating the information of individuals in the Central Identities Data Repository, omitting and deactivating an aadhaar number, sharing collected information with consent from the individual, establishing and maintaining the Central Identities Data Repository, specifying processes relating to data management, security protocols, levying and collecting fees for authentication, setting up a system of complaints for aggrieved individuals, calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of the proposed legislation of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act, entering into a Memorandum of Understanding or agreement with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or performing authentication; and appoint by notification, such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions. ***Section 23***

Verification

Existing Provisions

- The UIDAI will be responsible for notifying regulations as to the verification of collected information. ***Rule 23(a)***

ITA Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011[lxv]

4.17. The Personal Information Security Rules were notified in April 2011 and serve as the most comprehensive form of data protection in India. The Rules prescribe procedures and protocol by which body corporate must adhere to. The Rules can be brought in line with the National Privacy Principles through the following changes:

1. Notice

Existing Provisions

- **Privacy Policy:** Anybody corporate that collects, receives, possesses, stores, deals, or handles information must provide a privacy policy that provides for clear and easily accessible statements of its practices and policies, type of personal or sensitive personal data or information collected, purpose of collection and usage of such information, disclosure of information, and reasonable security practices and procedures. ***Rule 4***
- **During Collection**: While collecting information directly from the person concerned the body corporate shall take steps to ensure that the individual knows that the information is being collected, the purpose for which the information is being collected, the intended recipients of the information, the name and address of the agency collecting the information and the agency that will retain the information. ***Rule 5(3)***

Missing Provisions

- **Data Breach**: If a data breach occurs, affected individuals must be notified immediately.
- **Legal Access**: If information is legally accessed, the access must be notified at the close of the investigation.
- **Change in privacy policy**: Any changes in a body corporate privacy policy should be notified to the public and the individual.
- **Process to access and correct**: At the time of collection body corporates must provide notice of the processes available to data subjects to access and correct their own personal information.

2. Choice & Consent

Existing Provisions

- **Individual Consent:** Body corporates must obtain consent in writing through letter or Fax, or email from the provider of the sensitive personal data or information regarding purpose of usage before collection. ***Rule 5(1)***
- **Right to withdraw and opt in/opt out**: Prior to collection of information, body corporate must provide the individual not to provide the data sought. The provider of information will have the right to withdraw consent at any time while availing services. ***Rule 5(7)***

Missing Provisions

- **Mandatory provision:** When provision of information is mandated by is should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within one year if published in public databases.

3. Collection Limitation

Existing Provisions

- **Necessary & Relevant**: Body corporate shall not collect sensitive personal data unless the information is collected for a lawful purpose connected with a function or activity of the body corporate. The collection of sensitive personal data is considered necessary for the purpose. ***Rule 5(2)***

4. Purpose Limitation

Existing Provisions

- **Definition of Sensitive Personal Data:** password, financial information such as Bank account or credit card or debit card or other payment instrument details, physical, physiological and mental health conditions, sexual orientation, medical records and history, biometric information, any detail relating to the above as provided to body corporate for providing service, any of this information received by body corporate for processing, stored or processed under lawful contract. Any information that is available or accessible in public domain or furnished under the Right to Information Act, 2005 will not be regarded as sensitive personal data. ***Rule 3***
- **Retention:** The Body Corporate holding sensitive personal data will not retain that information for longer than is required for the purposes for which the information may be lawfully used or is required under any other law in force. ***Rule 5(4)***
- **Use:** The information collected will be used for the purpose for which it has been collected. ***Rule 5(5)***

Missing Provisions

- **Adequate and Relevant:** Personal data collected and processed by an organization must be adequate and relevant to the purposes for which they are processed.
- **Change in purpose:** If there is a change in purpose, this must be notified to the data subject.
- **Destruction:** After personal information has been used in accordance with the identified purpose, it must be destroyed as per the identified procedures.
- **Data Retention:** Data retention mandates by the government should be in compliance with the National Privacy Principles.

5. Access & Correction

Existing Provisions

- **Access:** Body corporate must permit the providers of information, when requested, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible. ***Rule 5(6)***

Missing Provisions:

- **Confirmation of personal information**: Data subjects should be able to confirm that an organization holds or is processing information about them.
- **Copy of personal information:** Data subjects should be able to obtain a copy of the personal data undergoing processing.
- **Limitation to Access:** The information may not be given or access permitted if it is not possible to do so without disclosing information about another person unless that persona has consented to the disclosure.

6. Disclosure of Information

Existing Provisions

- **Consent for Disclosure**: Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, unless disclosure has been agreed to by contract or is necessary by legal obligation. ***Rule 6***
- **Prohibition on publishing:** The body corporate will not publish the sensitive personal data or information. ***Rule 6(3)***
- **Non-disclosure:** The third party receiving the sensitive personal data will not disclose it further. ***Rule 6(4)***
- **Transfer of Information**: A body corporate may transfer sensitive personal data to any body, organization, or country that ensures the same level of data protection. The transfer can only take place for the performance of a lawful contract or where the transfer has been consented to. ***Rule 7***

Missing Provisions

- **Notice of disclosure**: Body corporate must provide notice of disclosure to third parties.
- **Bound to Principles:** All third parties must be bound to the National Privacy Principles.

Conflicting Provisions

- **Authorized Agencies**: Information will be share with Government Agencies mandated under law without obtaining prior consent for the purposes of verification of identity, for prevention, detection, investigation including cyber incidents, prosecution, and punishments of offences. ***Rule 6***

7. Security

Existing Provisions

- **Security standards:** A body corporate or person must have a comprehensive documented information security program and information security policies that contain managerial, technical, operational, and physical security control measures. In the event of a breach, the body corporate must be able to demonstrate that they have implemented security control measures. This includes being IS/ISO/IEC 27001 compliant. ***Rule 8(1)***
- **Audit:** On any annual basis the body corporate must undergo an audit of his/her reasonable security practices. ***Rule 8(4)***

8. Openness

Missing Provisions

Transparency: Body corporate must make available to the public information regarding the steps taken to ensure compliance with the National Privacy Principles

9. Accountability

Existing Provisions

- **System of Complaints**: Body Corporates must address any discrepancies and grievances of their provider of the information with respect to the processing of information in a time bound manner. To achieve this, a Grievance Officer must be appointed to address these grievances. ***Rule 5(9)***

Missing Provisions

- **External verification:** All processes related to the handling of sensitive personal information [in addition to security systems] should undergo external verification on a regular basis.
- **Support to Privacy Commissioner**: Body corporate should be held responsible for giving support to the Privacy Commissioner and complying with general/specific orders of the privacy commissioner.

10. Verification

Existing Provisions:

- **Liability of accuracy:** A body corporate is not responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information. ***Rule 5(6)***

Chapter 5: The Regulatory Framework

Ambit

5.1. The Privacy Act should put into place a regulatory framework for both public and private sector organisations. The ambit of the privacy legislation will extend to data being processed within India, and data that originated in India, even when it is transferred internationally. To do this the Act should establish the offices of the privacy commissioner. Additionally, the Act should enable a system of co-regulation through self-regulating organizations and their member organizations. These bodies should each play a distinct role in implementing the provisions of the Act. The Privacy Act should establish offenses and penalties, and list exceptions to the right of privacy. Any exception should be necessary in a democratic society, proportional, and in accordance with laws in force. The framework should enable quick redress by allowing individuals to resolve their complaints through alternative dispute mechanisms, the Privacy Commissioner, or the Courts. Once the Privacy Act is approved by Parliament, the regulatory bodies in the Act should be accountable to Parliament. The salient features of such a framework are:

- **Privacy Commissioners:** The regime will consist of privacy commissioners at the Central and Regional levels. An individual no less than a retired Supreme Court judge will be appointed as the Central level privacy commissioner. An individual no less than a retired High Court Judge will be appointed as the Regional level commissioner. The Central Office of the commissioner will be held accountable to Parliament. To accomplish this, the Privacy Commissioner will submit a report on an annual basis to Parliament that will contain all relevant statistics and information regarding its functioning. This report should include statistics related to complaints received and the data breaches of fined organisations. The commissioners will also have powers to investigate class action complaints or complaints received from individuals. Investigative powers of the commissioners will include the power to examine and call documents, examine witnesses, and compel appearances. The Commissioner should investigate data controllers on receiving complaints from data subjects, or *suo motu*, if such a cause arises. The commissioner will have the discretion to order privacy impact assessments. Aggrieved individuals or organisations cannot appeal fines on data controllers once they have been issued by the privacy commissioner, but individuals can appeal the commissioners' initial determination that a company was not in violation. If the privacy commissioner feels that it is necessary, it may take a case to the court. With respect to interception/access, audio & video recordings, the use of personal identifiers, and the use of bodily or genetic material, the Commissioner may exercise broad oversight functions.

  Privacy commissioners will also have the power to periodically review the working and functionality of the Privacy Act, and will have the ability to recommend alterations, consult with stakeholders, and selectively assess new legislation with privacy implications from a privacy perspective, prior to its passage. The privacy commissioners will also have the responsibility of approving codes of conduct created by industry level SRO's for conformance with privacy principles and clarifying, interpreting, and advising on the national level privacy principles.
- **Courts:** Individuals will have the option of taking a complaint directly to the courts, which will act as an alternative route of redress separate from the commissioner. The complaints can be related to a data breach or violation or physical privacy violation,

Complaints can be issued to a district level court, high level court, and to the Supreme Court.

- **SROs, co-regulation:** The Privacy Act will put in place a system of co-regulation that will give SROs at the industry level the choice to develop privacy standards, and at the same time will create a baseline legal framework that protects and enforces an individual's right to physical and informational privacy; these standards shall not be lower than those set in the Nation Privacy Principles. SROs that choose not to develop industry level privacy standards will be held accountable to the national level privacy principles. Co-regulation thus allows for both high level principles to be achieved and for specific privacy standards to be enforced. All principles developed by industry must be approved by the appropriate privacy commissioner, and the commissioner will have the power to enforce the agreed-upon standards, thus creating a system of co-regulation. SROs will be responsible for appointing an ombudsman to receive and handle complaints, and will be responsible for promoting education and awareness of sector specific privacy standards.

  Data Controllers and Privacy Officers: Every organization which determines the purposes and means of processing personal information will be considered a data controller. . Data controllers will be responsible for carrying out the processing of data in accordance with sectoral privacy standards or the national privacy principles. If a particular sector/industry does not have an SRO, then data controllers from that sector/industry will have to comply with the National Privacy Principles supplemented by any specific norms/standards prescribed by the Privacy Commissioner. These norms/standards may include the appointment of an organisational level privacy officer for complaints to be raised to and resolved. The appointment of privacy officers is meant to reduce case pendency in courts and at the regulators' office as well as to provide quick remedy/relief to consumers and citizens.

Exceptions to the right to privacy

5.2. The following exceptions may be considered to right to privacy:

- National Security
- Public order
- Disclosure in public interest
- Prevention, detection, investigation, and prosecution of criminal offences
- Protection of the individual or of the rights and freedoms of others

5.3. However, the following principles to the above exceptions must apply to measure the extent and validity of the exception to the right:

- **Proportionality**: The limitation should be in proportion to the harm that has been caused or will be caused and the objective of the limitation.
- **Legality**: The limitation should be in accordance with the laws in force
- **Necessary in a democratic state:** The limitation should extend only to that that is necessary in a democratic state.

5.4. Other exceptions that may be considered include:

- Historical or scientific research
- Journalistic purposes

Complaints

5.5. The individual, international data provider, whistle blower, auditor, commissioner, and public prosecutor/law enforcement will have the ability to submit complaints to organizations, SROs, privacy commissioners, or the courts. The system of complaints will be as follows:

a. **Alternative Dispute Resolution mechanisms**: Alternative dispute resolution (ADRs) mechanisms are the first level of redress available to individuals and will be implemented by SROs in specified verticals and by organisations. ADRs should be the first place that individuals take their complaints. These mechanisms should be the initial step for resolution of a complaint, and will reduce cost and increase efficiency in the delivery of justice. ADRs should be used to reduce pendency at courts and at the office of the commissioner. The Bill must recognize and encourage the use of alternative dispute resolution mechanisms to reduce the workload at the commissioner and court level.
b. **The Central & Regional level commissioner**: If a complaint is brought to the Central or Regional level commissioner, the commissioner will decide if the organisation was in violation, and if so, the extent of the fine. Fines issued by a Commissioner cannot be appealed, but decisions that the organisation was in violation can be appealed. Compensation to the individual cannot be granted by the Commissioner, and must instead be granted by the courts. The Commissioner can personally take a case to the courts if so required.
c. **Court:** The individual can take a complaint to the court and seek compensation for the harm caused by the violation. This includes harm caused by data breach, or a violation of physical privacy. A complaint can be issued to a district level court, high court, or the Supreme Court of India. If a Court wishes to undertake additional investigation, it must do so via the police. Courts can issue compensation to individuals, levy fines on organisations, and order imprisonment. Any person, who suffers damages caused by non-compliance with the principles or any obligation under the Act, should be entitled to remedy from the data controller to the full extent of the damages suffered. Remedies available to the individual include directive or injunctive orders, compensation, or punitive actions. Actors that can be held liable by individuals include data controllers, privacy officers, organization directors, agency directors, and heads of Governmental departments.
d. **Remedies:** Any person, who suffers damages caused by non-compliance with the principles or any obligation under the Act, should be entitled to remedy from the data controller to the full extent of the damages suffered. Actors that can be held liable by individuals include data controllers, organization directors, agency directors, and heads of Governmental departments.

Offences and Penalties

5.6. The infringement of any provision under the Act will constitute as an offence by which individuals may seek compensation for, and organizations/bodies held accountable to.

5.7. As found in the UK Data Protection Act, and the Australian Privacy Act the following could be broad offences under the Act:

- **Non-compliance with the privacy principles**

- **Unlawful collection, processing, sharing/disclosure, access, and use of personal data**
- **Obstruction of commissioner**
  - Failure to comply with notification issued by commissioner
  - Processing data after receiving a notification
  - Failure to appear before commissioner
  - Failure to produce documents requested by commissioner
  - Sending report to commissioner with false or misleading information

Chapter 6: The Multiple Dimensions of Privacy

A. Interception and Access

6.1. Interception/access to communication data is frequently practiced by governments across the globe, but when carried out without comprehensive privacy safeguards in place, can violate individual privacy. Internationally, best practices regarding interception and access have included appointment of an Interception of Communications Commissioner[lxvi], court order for interception[lxvii], criminalization of unauthorized disclosure of intercepted material and orders.[lxviii]

6.2. In India interception/access is addressed by two legislation, the Indian Telegraph Act (TA) 1885 and the Information Technology Act (ITA) 2008. Each Act prescribes varying standards and procedures for interception through Rules, thus creating interception regimes that have both similar and varying standards and procedures. Broad similarities between the regimes include that authorization for interception must be based on executive orders, orders for interception must be reviewed by an overseeing committee, all interception orders must contain similar specified information, and every agency intercepting communications must establish similar procedures for the oversight, processing, conducting, and security of the interception. In addition to the TA and the ITA, the UASL and ISP licenses establish the ways in which service providers must assist the government in carrying out an interception through systemic access and proactive disclosure. Though the licenses are rooted in the Telegraph Act, it is unclear to what degree the licenses are in compliance with the safeguards established in this legislation.

6.3. Differences between the regimes (legislation and licenses) range from:

- Permitted grounds for surveillance: for example investigation of an offense vs. investigation of any cognizable offense etc.
- Type of interception that is permitted to be undertaken: for example monitoring vs. tracking vs. intercepting etc.,
- Type and granularity of information that can be intercepted: for example communications vs. encrypted information vs. location data etc.
- Degree of assistance that authorized agencies can demand from service providers: for example in house facilities vs. technical assistance, vs. proactive disclosure of prescribed information etc
- Destruction and retention requirements of intercepted material: for example six months vs. one year vs. as long is necessary etc.

6.4. These differences have created an unclear regulatory regime that is inconsistent, nontransparent, prone to misuse, and that does not provide remedy or compensation to aggrieved individuals. The regime does not require judicial oversight or authorization, it is unclear which agencies are legally authorized to undertake interception/access, systematic access or proactive disclosure of communications and classes of data is not prohibited, agencies are not required to be transparent to the public regarding the effectiveness and cost of each intercept, interception/access is permitted for even minor offenses, there is no requirement for standardization of orders, there are no additional safeguards for when interceptions/access invade individual's privacy beyond the targeted subject, and the individual is never notified that an interception/access took place, even after the close of the investigation. Furthermore, the regime is silent on certain categories of data – such as location data. The differences between the regimes, and the policy gaps

that exist, facilitate violations of privacy as broad interception/access is permitted to a wide category of information, during vague and changing circumstances, without adequate safeguards in place.

6.5. When compared to the National Privacy Principles identified by the committee, each legislation (not licenses) in the current interception regime fully or partially upholds only four out of the nine principles.[1] These include:

- **Accountability**: Interception orders must be sent for review by the designated committee, the officer to whom information relating to interceptions can be disclosed must be specified, security agencies and service providers must appoint nodal officers responsible for the receipt and handling of interception orders
- **Collection limitation:** Reasons for interception order must be specified and recorded in writing, the provisions establish conditions for authorization by the competent authority, all interceptions can only be in force for a period of sixty days and renewed for a period which can extend to 180 days. Records of interception must be destroyed by security agencies after six months or nine months, and service providers must destroy records after two months or six months.
- **Purpose limitation:** Before an order for interception is issued, all other means of obtaining the information must be considered, and use of intercepted material must be limited to an investigation.
- **Security:** Intermediaries must provide an internal check to ensure the security, confidentiality, and privacy of intercepted material, and intermediaries are held legally responsible for any unauthorized access or disclosure of intercepted material

6.6. Principles that may need to be addressed and strengthened in the regime include openness, accountability, purpose limitation, collection limitation, disclosure to third parties, and notice. In the instance of interception/access the National Privacy Principles may be affected as follows:

- **Consent and Choice**: Individuals may not be given the choice of being monitored, and consent from the individual may not be required for an interception to take place.
- **Access and Correction**: Individuals may not be able to access interception records pertaining to them during an investigation.
- **Notice**: Authorized agencies may be required to provide notice of legal access after an investigation is closed.

B. Audio and Video Recording

6.7. Audio & Video recording refers to the use of electronic recording devices. This can range from the employment of CCTV cameras, the generic use of recording devices found in widely available technologies, like mobile cameras, recording devices used by journalists and investigators for sting operations, and the use of satellites and mapping devices by data controllers - like Google Earth and Street View projects, and the use of unmanned aerial vehicles. These technologies are widely used by individuals, organizations, and governments, but when carried out without comprehensive privacy safeguards in place, can violate individual privacy. Internationally, best practices regarding the use of electronic devices have included: ensuring effective administration of the equipment, ensuring proper security measures are placed over recorded material,

[1] See Annex VIII for complete analysis of the interception regime and the National Privacy Principles

limiting the disclosure of recorded material to ways consistent with the purpose of the use, and when applicable providing public notice of the use of the devices.[lxix]

6.8. Currently in India the use of audio and video recording devices is unregulated, though there have been attempts to address the use of these devices. In 2006 the Mobile Camera Phone Users (Code of Conduct) Bill 2006 was introduced in Parliament, but has lapsed, and in 2010 the Right to Privacy Bill was proposed in Parliament, but has not been passed. The Mobile Camera Phone Users (Code of Conduct) Bill proposed to create a code of conduct regulating the use of mobile camera phones in public places. Among other things the Bill proposed requiring that all manufactures build camera phones that either flash a light or emit a sound when being used, regulate where camera phones are permitted to be used, and what procedures need to be adhered to when using mobile phones in public such as taking consent and ensuring that the individual is aware that a picture will be taken. Similarly, the Right to Privacy Bill 2010 proposed to prohibit the use of cellular phones with built in cameras unless the camera produces that do not emit a sound of at least 65 decibels and flash a light. Digital recordings of individuals are prohibited without consent if the recording is of an unclothed body part, the recording is in a public place, or of a couple in a private place – with the intent of blackmail or making commercial gains. Neither of the Bills were approved by Parliament. Thus, the lack of regulation has led to a situation where it is unclear when and where recording devices built into technologies can be employed, and how the recorded information can subsequently be used i.e. can it be uploaded to Face book or YouTube without prior permission.

6.9. In India private and public organizations use audio & video recording devices, namely CCTVs, to monitor premises and detect unlawful activities in public spaces, yet there are no clear regulations as to the circumstance and manner in which devices such as CCTVs can be employed. In some cases individuals are notified that a device is being used to monitor the premise, and in other cases, no notice is given, and the individual is left unaware of the recording. After the recording takes place it is not clear what happens to it. It can be assumed that in some cases organizations simply store the information, while news items show that in other cases private establishments make CCTV camera feeds available to police in real-time.[lxx] News items also reveal that the police often encourage the installment of CCTVs[lxxi], and use the recordings during an investigation or to prevent crime.[lxxii] The lack of established procedure over the use of audio & video recording devices has resulted in the unclear demarcation between police and civic devices, varying standards of device use between organizations, and unclear use and access to recorded information. This not only creates the potential for a violation of privacy to take place through the misuse of recording devices or the misuse of recorded information, but also creates a situation where the individual is not aware that his/her privacy was violated.

6.10. The use of electronic recording devices by journalists or whistle blowers for the purposes of conducting sting operations is also not addressed in India. Though in 2010 the Public Interest Disclosure and Protection to Persons Making the Disclosures Bill was proposed for the purpose of creating a system for leaks and complaints to be issued, the Bill was never passed, and the Press Council Act 1978 does not directly address the use of recording devices during sting operations.

6.11. When these technologies are employed by data controllers the National Privacy Principles should apply. When applied to the use of audio & video recording equipment

by private organizations for monitoring purposes, the National Privacy Principles may be affected as follows:

- **Collection limitation**: These devices broadly monitor public spaces and it may not be possible to limit the type and quantity of information collected.
- **Access & correction:** Individuals may not be able to access information recorded about them, because it would cause undue overhead for organizations. An exception to this may be if individuals can demonstrate that access to the information is necessary and relevant.
- **Consent & choice***:* It should be understood that when an individual enters a space that has provided public notice of audio and video recording, they are consenting to being monitored.

6.12. In the context of exceptional circumstances, the use audio & video recording may not be regulated by the National Privacy Principles except in the following ways:

- **Accountability:** Individuals using devices must be accountable to an overseeing body to ensure that the circumstances are exceptional, and that the uses of the devices are not abused.
- **Security:** Recorded information must be secured to ensure that unauthorized use and disclosure does not take place.
- **Collection Limitation**: Information pertaining only to the exceptional circumstance should be collected.
- **Purpose Limitation:** Collected information should only be used for purposes related to the exceptional circumstance.
- **Notice:** If an individual is recorded, the individual should be notified after the investigation, exposure etc. is completed.

6.13. In the context of recording devices being built into widely available technologies, manufactures may be required to build the privacy principle of purpose limitation into the design of technologies through features that only allow the technology to be used in a specific manner. It should not be possible for users to turn these features off.

C. Access and Use of Personal Identifiers

6.14. Data controllers are using personal identifiers to converge databases, track individuals, and create comprehensive profiles about consumers and citizens. When carried out without comprehensive privacy safeguards, this practice can violate individual privacy. Internationally, the use of personal identifiers across databases and the convergence of information related to personal identifiers has not been comprehensively addressed. Many countries discourage the practice, but do not legally regulate the practice. For example, in the United States organisations are encouraged to only collect the Social Security Number (SNN) when necessary. Other safeguards include requiring that organisations encrypt the SSN upon collection, and if there is a breach related to the ssn, the Federal Trade Commission has the power to sue the company.

6.15. Personal identifiers are a type of personal information, but unlike personal information like ‘sexual orientation’, personal identifiers can uniquely identify an individual, and can reveal any additional information about an individual that was attached to the identifier or generated by the use of the identifier. Personal identifiers, like UID number, Personal Account Number, and Passport number, ubiquitously serve as personal identifiers for individuals in India, as public and private organizations now mandate them to complete transactions and provide services. As a result of this practice,

centralized and decentralized databases that contain detailed records of individuals and their transactions are being converged by organizations and bodies on an adhoc basis. The amount and granularity of information that can be converged through the use of these personal identifiers makes it possible for comprehensive profiles to be created of individuals and track individuals across databases via their personal identifier.

6.16. In India the access and use of personal identifiers for tracking and convergence purposes is not addressed by the legislations that legally establishes personal identifiers (The Passport Act, the UID Bill, the Indian Tax Act etc.), and is not addressed at the organizational or departmental level through policy. Thus, it is unclear if access is taking place in accordance with laws in force, and what standards are in place to prevent the unauthorized disclosure/access/use of personal identifiers. Therefore, it is not clear which organizations/bodies are legally collecting and storing personal identifiers, for what purposes, who is accessing data based on personal identifiers, how personal identifiers are being secured, how long personal identifiers are being retained, and if/how the personal identifiers are deleted. This creates a situation where governmental and private sector organizations can potentially access and use information directly or indirectly connected to, or generated by personal identifiers for multiple purposes without explicit authorization, and without the individual being aware or consenting to such access and use.

6.17. Furthermore, when legal access to personal identifiers takes place, the concerned individual is not notified as to which personal identifier was accessed via which database, for what period of time, for what purpose, and for how long this accessed information is retained. If a violation of privacy takes place through unauthorized access or misuse of accessed information, it is unclear how the individual will seek redress and compensation, and organizations that misuse personal identifiers cannot be held legally accountable.

6.18. In order to ensure that the practice of accessing personal information using personal identifiers is uniform across India, and that organizations adhere to privacy safeguards that protect the privacy of individuals, the use of personal identifiers across databases should be in compliance with the National Privacy Principles and should conform to the principles of proportionality, legality and necessary in a democratic society. All National Privacy Principles will apply to private sector organisations collecting, storing, and accessing personal identifiers. Regarding the collection, storage, and access of personal identifiers by authorized governmental agencies, the National Privacy Principles may be affected as follows:

- *Choice & Consent:* Individuals may not have a choice to be traced across databases for investigation purposes, and authorized agencies may not be required to take individual consent before tracing personal identifiers across databases. When authorized agencies use personal identifier without taking consent this should in accordance with law and in keeping the National Privacy Principles
- *Notice*: The authorized agency may only be required to give notice of the legal access to the personal identifier, after the completion of the investigation. When personal identifiers are accessed by authorized agencies they should be used in accordance with law and in keeping with the privacy principles.
- *Purpose Limitation*: The purpose for which personal identifiers are used cannot always be limited, as platforms may mandate the use of personal identifiers for different transactions and for different purposes. Furthermore, if databases containing personal identifiers are converged, the personal identifier may not be used in accordance to the original purposes that it was collected for. If the use of a

personal identifier is not used for its original purpose, it should still be used in accordance with law and in keeping with the national privacy principles.

D. Bodily and Genetic Material

6.19. The use of bodily and genetic material is widely used by individuals, governments, and law enforcement for reasons ranging from conducting paternity tests, to identifying a victim or a criminal, but when used without comprehensive privacy safeguards or constitutional protections in place, can violate individual privacy. Internationally, best practices regarding the use of bodily and genetic material have included: taking consent from individuals when possible (victim, for exculpation etc), requiring that law enforcement have a court order for the collection of samples, providing information to all persons from whom a sample was taken, and storing the samples of convicted persons separate from other samples.[lxxiii]

6.20. Regulation over the collection, use, analysis, and storage of identifying bodily samples is limited in India. In 2005 section 53 of the Code of Criminal Procedure (CrPc) was amended to enable the collection of medical details from accused persons upon their arrest if there are "reasonable grounds for believing" that such examination will afford evidence as to the crime. Medical details that can be collected and examined include "blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case." Besides these provisions, any collection, analysis, storage, access, and retention of genetic material is presumed to be done outside the scope of regulation, and completed in a manner which does not recognize the sensitive nature of this information.

6.21. In 2007 a Draft DNA Profiling Bill was created to establish a centralized DNA bank that would incorporate information from existing DNA databanks, and store DNA records of suspects, offenders, missing persons, and 'volunteers. Though the Bill creates some standards for privacy, many safeguards are missing. News items reveal that private labs process DNA samples for purposes such as paternity testing[lxxiv], and public labs process DNA for forensic purposes.[lxxv] The provisions of the CrPc, and the lack of more specific legislation has created a situation where the privacy of individuals is put at risk through the potential of unauthorized or inaccurate collection and use of bodily and genetic material.

6.22. According to existing provisions in the CrPc it is not clear beyond law enforcement, what bodies are permitted to collect, process, and store what types of bodily and genetic samples, and for what purposes. Collecting bodies are not legally required to follow an approved procedure for collection, or to provide individuals with the choice at the time of collection, take consent from the individuals at the time of collection or processing, or provide individual notice of the collection, processing, or use of bodily and genetic material. Laboratories processing and storing bodily and genetic material are not legally required to provide accessible notices of the persons or organizations to which personal information regarding the collected and processed samples may be disclosed, how information will be stored, how long information will be retained, when information will be deleted/destroyed, and the security safeguards established to secure the personal information. There is also no established legal procedure for individuals to access and correct stored information, and if unauthorized access or disclosure of bodily or genetic material takes place, there is no procedure to hold collecting and processing bodies

legally liable. Furthermore, though bodily and genetic material can be collected and used for varying purposes (identifying a victim vs. identifying a convicted criminal) it is not clear if each category of sample is stored separately, and if the databases storing the samples are independent of law enforcement agencies.

6.23. When applied to practices around the use of bodily and genetic material, the National Privacy Principles may be affected as follows:

- *Notice:* There are circumstances where at the point of collection, it may not be possible to provide notice to the individual, for example when a sample is collected from a suspect at a crime scene or from a victim.
- *Choice & consent:* There are circumstances where it may not be possible for consent to be taken at the time of collection of the sample, for example from a missing individual or victim unable to communicate consent.

Summary of Recommendations

7.1. On the basis of the analysis in the chapters above on the diverse aspects germane to privacy regulation in India, the Group makes the following recommendations regarding a proposed framework for a Privacy Act for India, which the Department of Personnel and Training, Government of India, may be pleased to consider:

Objectives and Scope

7.2. The Indian Privacy Act should:

- Clarify its ambit and definitions;
- Specify the constitutional basis of the right to privacy;
- State National Privacy Principles which can be used to harmonise legislation, policy, and practices including but not limited to interception, the use of personal identifiers, the use of audio and video recordings, the use of bodily and genetic material, and the use of personal information by the government and the private sector;
- List additional exemptions necessary in the context of privacy and explain the necessary measures to weigh exemptions and limitations to the right of privacy against;
- Articulate an enforcement regime including establishing the office of the Privacy Commissioner at the regional and central levels, defining the role of SRO's and co-regulation, and creating a system of complaints and redressal for aggrieved individuals;
- Prescribe safeguards for physical privacy including search and seizure;
- Enumerate offences, associated remedies, and penalties;

Ambit and Definitions

7.3. As the concept of privacy is constantly changing based on context, societal norms, and emerging technology, the Privacy Act should be technology and sector neutral. Because of the dynamic nature of privacy, the Privacy Act should create a right to privacy that is applicable to all situations and does not require that a 'reasonable expectation' be present, for the right to be evoked. This is to ensure that when seeking redress, the individual is not required to prove that he/she had a 'reasonable expectation of privacy' before being awarded remedy.

7.4. The Act should take into consideration that personal information can be contextual – the same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another data controller- e.g.- possession of license plate number in the hands of an insurance company can be considered as personal information but the same plate number in the tape of a security camera in a petrol station will not be personal information, as the station has to take considerable efforts for determining the identity of the person. The definition of personal information therefore should be at high level (not prescriptive) giving space for various contexts.

7.5. Further, the Privacy Act should broadly define and harmonize with existing definitions under laws in force, Sensitive Personal Information, Personally Identifying Information, and Indirectly Identifiable Information. The Privacy Act should establish National Level Privacy Principles with respect to the collection, processing, storage,

access, retention, destruction, and anonymization of this information. When Sensitive Personal Data is processed, the National Privacy Principles should be legislated more stringently. Existing and emerging legislation, policy, and projects should be brought into compliance with the National Privacy Principles. The Act should create offences, enforce penalties, and provide remedies for related violations.

7.6. The Privacy Act should extend the right of privacy to individuals, and bring under its regulation data controllers, which includes all body corporates and public/governmental bodies and organizations. The Act should extend the right to privacy to all persons in India, all data that is processed by any company or equipment located in India, and all data that has originated in India.

7.7. The Privacy Act should clarify that publication of personal data for artistic and journalistic purposes in public interest, use of personal information for household purposes, and disclosure of information as required by the Right to Information Act should not constitute an infringement of Privacy.

International Obligations

7.8. India has signed and ratified many international treaties and agreements that recognize and create an obligation to protect the privacy of individuals. In 1979 India ratified the International Covenant on Civil and Political Rights (ICCPR), which came into force in 1976. Article 17 of the Covenant articulates a right to privacy, stating "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation, and that everyone has the right to the protection of the law against such interference or attacks." India is also a member of the General Agreement on Trade in Services, which under Article XIV creates an exception for privacy, stating that "nothing in the agreement shall be construed to prevent the adoption or enforcement of the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[2] This same exception is reflected in the World Trade Organization services agreement, to which India is also a member.[3]

Constitutional Basis

7.9. The Privacy Act must articulate the constitutional basis of privacy as a fundamental right deriving from Article 21 of the Constitution of India.

Exceptions to the Right

7.10. The following exceptions may be considered to right to privacy:

- National Security
- Public order
- Disclosure in public interest
- Prevention, detection, investigation, and prosecution of criminal offences.
- Protection of the individual or of the rights and freedoms of others;

7.11. However, the following principles to the above exceptions must apply to measure the extent and validity of the exception to the right:

[2]http://www.worldtradelaw.net/uragreements/gats.pdf

[3]http://www.wto.org/english/tratop_e/serv_e/2-obdis_e.htm

- **Proportionality**: The limitation should be in proportion to the harm that has been caused or will be caused and the objective of the limitation.
- **Legality**: The limitation should be in accordance with the laws in force
- **Necessary in a democratic state:** The limitation should extend only to that that is necessary in a democratic state.

7.12. Other exceptions that may be considered include:

- Historical or scientific research
- Journalistic purposes

Harmonisation with existing laws

7.13. In India, there exist at least 50 laws, rules, regulations and executive orders that articulate privacy principles, practices, and related offences for different verticals such as finance, health, e-governance, telecommunication etc.[4] The Privacy Act will be used to harmonize, but not homogenize these different policy documents to ensure that there is consistency, and compliance with the defined National Privacy Principles. The Privacy Act should be clear and concise to most effectively accomplish this overriding effect. To do this, the Privacy Act should only define the National Privacy Principles, and allow specific sectors [such as health] to develop, or use already developed privacy standards. Once the Privacy Act becomes law – other laws with privacy implications may be amended to ensure that sectoral variations are retained, but that broad harmonization and compliance with the National Privacy Principles takes place. If any other legislation provides more extensive protections than those set out by the Privacy Act, than the more extensive protections should apply.

National Privacy Principles & SRO Privacy Standards

7.14. The Privacy Act will articulate National Privacy Principles. The principles will extend and be binding to all private/public data controllers. The principles must establish:

(1) Safeguards and procedures over the collection, processing, storage, retention, access, disclosure, destruction, and anonymization of sensitive personal information, personal identifiable information, and identifiable information.
(2) Rights of the data subject in relation to their Sensitive Personal Information, Personal Identifiable Information, and Identifiable Information.

7.15. The principles will place an obligation on data controllers to put in place safeguards and procedures that will enable and ensure these protections and rights. The principles must be applicable to any information concerning an identified or identifiable natural person. Existing and emerging legislation, practices, and procedures should be brought into compliance with the National Privacy Principles.

7.16. Alongside the National Privacy Principles, self regulating bodies will have the option of developing industry specific privacy standards that would be in conformity with the National Privacy Principles, which should be approved by a Privacy Commissioner. The Privacy Commissioner should have the power to enforce the agreed-upon standards, thus creating a system of co-regulation. If SROs do not develop standards, their member organisations shall be required to adhere to the National Privacy Principles.

[4] See Annex VIII

7.17. The National Privacy Principles should require:

Principle 1: Notice

A data controller shall give simple to understand notice of its information practices to all individuals, in clear and concise language, before any personal information is collected from them. Such notices should include:

a) During Collection
- What personal information is being collected;
- Purposes for which personal information is being collected;
- Uses of collected personal information;
- Whether or not personal information may be disclosed to third persons;
- Security safeguards established by the data controller in relation to the personal information;
- Processes available to data subjects to access and correct their own personal information;
- Contact details of the privacy officers and SRO ombudsmen for filing complaints.

b) Other Notices
- Data breaches must be notified to affected individuals and the commissioner when applicable.
- Individuals must be notified of any legal access to their personal information after the purposes of the access have been met.
- Individuals must be notified of changes in the data controller's privacy policy.
- Any other information deemed necessary by the appropriate authority in the interest of the privacy of data subjects.

Principle 2: Choice and Consent

A data controller shall give individuals choices (opt-in/opt-out) with regard to providing their personal information, and take individual consent only after providing notice of its information practices. Only after consent has been taken will the data controller collect, process, use, or disclose such information to third parties, except in the case of authorized agencies. When provision of information is mandated by law, it should be in compliance with all other National Privacy Principles. Information collected on a mandatory basis should be anonymized within a reasonable timeframe if published in public databases. As long as the additional transactions are performed within the purpose limitation, fresh consent will not be required.

The data subject shall, at any time while availing the services or otherwise, also have an option to withdraw his/her consent given earlier to the data controller. In such cases the data controller shall have the option not to provide goods or services for which the said information was sought if such information is necessary for providing the goods or services. In exceptional cases, where it is not possible to provide the service with choice and consent, then choice and consent should not be required.

Principle 3: Collection Limitation

A data controller shall only collect personal information from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken. Such collection shall be through lawful and fair means.

Principle 4: Purpose Limitation

Personal data collected and processed by data controllers should be adequate and relevant to the purposes for which they are processed. A data controller shall collect, process, disclose, make available, or otherwise use personal information only for the purposes as stated in the notice after taking consent of individuals. If there is a change of purpose, this must be notified to the individual. After personal information has been used in accordance with the identified purpose it should be destroyed as per the identified procedures. Data retention mandates by the government should be in compliance with the National Privacy Principles.

Principle 5: Access and Correction

Individuals shall have access to personal information about them held by a data controller; shall be able to seek correction, amendments, or deletion such information where it is inaccurate; be able to confirm that a data controller holds or is processing information about them; be able to obtain from the data controller a copy of the personal data; . Access and correction to personal information may not be given by the data controller if it is not, despite best efforts, possible to do so without affecting the privacy rights of another person, unless that person has explicitly consented to disclosure.

Principle 6: Disclosure of Information

A data controller shall only disclose personal information to third parties after providing notice and seeking informed consent from the individual for such disclosure. Third parties are bound to adhere to relevant and applicable privacy principles. Disclosure for law enforcement purposes must be in accordance with the laws in force. Data controllers shall not publish or in any other way make public personal information, including personal sensitive information.

Principle 7: Security

A data controller shall secure personal information that they have either collected or have in their custody, by reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure [either accidental or incidental] or other reasonably foreseeable risks.

Principle 8: Openness

A data controller shall take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data they collect, in order to ensure compliance with the privacy principles, information regarding which shall be made in an intelligible form, using clear and plain language, available to all individuals.

Principle 9: Accountability

The data controller shall be accountable for complying with measures which give effect to the privacy principles. Such measures should include mechanisms to implement privacy policies; including tools, training, and education; external and internal audits, and requiring organizations or overseeing bodies extend all necessary support to the Privacy Commissioner and comply with the specific and general orders of the Privacy Commissioner.

Application of the National Privacy Principles:

7.18. The National Privacy Principles have been envisioned as being applicable across sectors, legislation, policy, projects, and bodies in order to broadly harmonize privacy protection in India and address and readily adapt to emerging and changing technologies and practices. For example, the National Privacy Principles could be applied to the following regimes and practices that currently do not adequately address privacy:

Interception and Access

7.19. At the moment, interception/access in India is addressed in two legislation, the Telegraph Act and the Information Technology Act. Each Act prescribes varying standards and procedures for interception through Rules, thus, creating similarities and differences in the Indian interception regimes. Broad similarities between the regimes include: authorization for interception must be based on executive orders, orders for interception must be reviewed by an overseeing committee, all interception orders must contain similar specified information, and every agency intercepting communications must establish similar procedures for oversight and security of the interception. Differences range from the permitted grounds for surveillance, the type of interception that is permitted to be undertaken (monitoring, tracking, intercepting etc.), the type and granularity of information that can be intercepted, the degree of assistance that authorized agencies can demand from service providers, and the destruction and retention requirements of intercepted material. These differences have created an unclear regulatory regime that is nontransparent, prone to misuse, and that does not provide remedy for aggrieved individuals. By requiring that each legislation be in compliance with the National Privacy Principles, the Principles should be used to harmonize the interception regime in India. See chapter 6 for detailed analysis of how the National Privacy Principles could apply to the current interception regime.

Video and Audio Recording

7.20. In India the use of video and audio recording devices are used by multiple stakeholders for various reasons including the public for entertainment reasons, journalists for investigation purposes, and private/ public organizations and law enforcement for crime detection purposes. Though there have been some attempts to create legal regulation over the use of video and audio recording devices by these stakeholders, including the Mobile Camera Phone Users (Code of Conduct) Bill 2006, Right to Privacy Bill 2012, and the Public Disclosure and Protection of Persons Making Disclosures Bill, there are no clear regulations as to the circumstance and manner in which these devices can be employed. This has resulted in a situation where it is unclear who is employing video and audio recording in public spaces, how recording is being conducted, and how collected recordings are being used. Any individual or public/private organization using video and audio recording equipment in India should be bound to do so in compliance with the National Privacy Principles. See chapter 6 for detailed analysis of how the National Privacy Principles could apply to the use of electronic audio and video recording devices.

Use of Personal Identifiers

7.21. The ubiquitous use of personal identifiers, like UID, PAN, and Passport, to complete transactions is taking place across India. As a result of this practice, centralized and decentralized databases that contain detailed records of individuals and their transactions are being converged by organizations and bodies on an adhoc basis. The amount and granularity of information that can be converged through the use of these personal identifiers makes it possible for comprehensive profiles to be created of individuals and track individuals across databases via their personal identifier. In India the use of personal identifiers across databases by third parties for tracing, convergence, or collation purposes is not addressed in the legislation that legally establishes the personal identifier [the UID Bill, Citizenship Act, the Passport Act, and the Indian Tax Act etc.] and is not addressed at the organizational or departmental level through policy. Thus, it is unclear if access is taking place in accordance with laws in force, and what standards are in place to prevent the unauthorized disclosure/access/use of personal identifiers. Therefore, it is not clear which organizations/bodies are legally collecting and storing personal identifiers, for what purposes, who is accessing data based on personal identifiers, how personal identifiers are being secured, how long personal identifiers are being retained, and if/how the personal identifiers are deleted. This creates a situation where governmental and private sector organizations can potentially access and use information directly or indirectly connected to, or generated by personal identifiers for multiple purposes without explicit authorization, and without the individual being aware or consenting to such access and use. The use of personal identifiers across databases should be in compliance with the National Privacy Principles. See chapter 6 for detailed analysis of how the National Privacy Principles could apply to the use of personal identifiers across databases.

Bodily and Genetic Material

7.22. Regulation over the collection, use, analysis, and storage of identifying bodily samples is limited in India. In 2005 section 53 of the Indian Code of Criminal Procedure (CrPc) was amended to enable the collection of medical details from accused persons upon their arrest if there are "*reasonable grounds for believing"* that such examination will afford evidence as to the crime. Medical details that can be collected and examined

include "*blood, blood stains, semen, swabs in case of sexual offences, sputum and sweat, hair samples and finger nail clippings by the use of modern and scientific techniques including DNA profiling and such other tests which the registered medical practitioner thinks necessary in a particular case."* Besides these provisions, any collection, analysis, storage, access, and retention of genetic material is taking place outside the scope of regulation and is being done in a manner which does not recognize the sensitive nature of this information. In 2007 a Draft DNA Profiling Bill was created to establish a centralized DNA bank that would incorporate information from existing DNA databanks, and store DNA records of suspects, offenders, missing persons, and 'volunteers. Though the Bill creates some standards for privacy, many safeguards are missing. The Bill is still pending in Parliament. Existing and newly developed protocols for the collection, use, analysis, storage, access, and retention of bodily and genetic material should be in compliance with the National Privacy Principles. See chapter 6 for detailed analysis of how the National Privacy Principles could apply to the use of Bodily and Genetic Material.

Legislation

7.23. There is a number of existing and emerging legislation and policy in India have provisions that either partially protect or conflict with the privacy of individuals. This has led to a situation where legal protection of privacy in India is scattered, inconsistent, and often leaves individual privacy unprotected. The National Privacy Principles can be applied to legislations and policy to ensure that the legal level of privacy protection in India. See chapter 4 for detailed analysis of how the National Privacy Principles could apply to various sectoral legislation.

Enforcement Regime

7.24. For the purposes of implementation and enforcement, the Privacy Act should establish the central office of the Privacy Commissioner, regional level privacy commissioners, self-regulating organizations [SRO's] at the industry level, and data controllers and privacy officers [if required] at the organisational level. For the purpose of issuing remedies and enforcing penalties the Privacy Act should involve the district level, high level, and Supreme Court. The Privacy Act should not establish a separate tribunal, or rely on an existing tribunal [such as found under the Information Technology Act] as there is a risk that the institution will not have the capacity to rule on a broad right of privacy.

Privacy Commissioners

7.25. The regulator should be called a Privacy Commissioner rather than a Data Protection Commissioner to follow the nomenclature, scope and intent of the statute. Unlike the Right to Information commissioners - there should be one national Commissioner and four regional Commissioners. The Commissioners will be the officers primarily responsible for enforcement of the Privacy Act. With respect to data protection, the commissioners should have the power to order privacy impact assessments on organisations, investigate complaints, and fine non-compliant data controllers. The Commissioners should have the power of investigation, including the power to summon documents, call and examine witnesses, and take a case to court if necessary. The Commissioner should investigate data controllers on receiving complaints from data subjects, or *suomotu*, if such a cause arises. The commissioner will have the discretion to order privacy impact assessments. The fines imposed by the Commissioner for violation

of the National Privacy Principles should be binding. Data controllers and individuals should have the right to appeal the decisions of the Commissioners. The Commissioner should have the power to approve the privacy standards which SRO's may have autonomously formulated in conformity with the National Privacy Principles. With respect to interception/access, audio & video recordings, the use of personal identifiers, and the use of bodily or genetic material, the Commissioner may exercise broad oversight functions. More generally, to ensure efficient and effective enforcement of the Privacy Act, Commissioners should collaborate with stakeholders including industry, civil society, and sector-specific regulatory bodies to ensure effective regulation, promote awareness of the Act, and play a key educative role in sensitizing the citizenry to privacy considerations.

Self-Regulating Organizations (SROs) and Co-regulation

7.26. Self-regulation and co-regulation will supplement the role played by the Privacy Commissioners. This is to ensure that appropriate policies are articulated, implemented, and enforced policies for a wide range of sectors/industries, and that the fast changing nature of technology is addressed by these policies. SROs will, in consultation, with their membership develop norms/standards for self-regulation in conformity with the NPP. From time to time the SRO will submit a sub-set of self-regulation norms/standards to the Privacy Commissioner for approval. Once approved, these norms/standards will create a co-regulatory framework. This means that the Privacy Commissioner will be able to investigate and sanction member data controllers for being in violation of the SRO co-regulatory norms. If a particular sector/industry does not have an SRO, then data controllers from that sector/industry will have to comply with the National Privacy Principles supplemented by any specific norms/standards prescribed by the Privacy Commissioner. These norms/standards may include the appointment of an organisational level privacy officer for complaints to be raised to and resolved. The SROs will also appoint a sector/industry wide ombudsman. The appointment of privacy officers and ombudsman are meant to reduce case pendency at courts and at the regulators' office as well as to provide quick remedy/relief to consumers and citizens.

The System of Complaints

7.27. The individual, international data provider, whistle blower, auditor, commissioner, and public prosecutor/law enforcement should have the ability to submit complaints to public/private data controllers, SRO's, privacy commissioners, or the courts. The system of complaints could be as follows:

a. **Alternative Dispute Resolution mechanisms**: Alternative dispute resolution (ADRs) mechanisms could be the first level of redress available to individuals and should be implemented by data controllers and SROs in specified verticals. If an individual has a complaint, they should approach the ombudsman at the data controller, and if not resolved, the individual should approach the SRO ombudsman. These mechanisms could reduce cost and increase efficiency in the delivery of justice, by reducing pendency at courts and at the office of the commissioner. To provide legitimacy to these mechanisms, the Privacy Act should recognize and encourage the use of alternative dispute resolution mechanisms.
b. **The Central & Regional level commissioner**: If a complaint is brought to the Central or Regional level commissioner, the commissioner should decide if the data controller was in violation, and if so, the extent of the fine. Data controllers and individuals should be able to appeal decisions issued by a commissioner.

Compensation to the individual should be granted by the courts instead of the Privacy Commissioner. The Commissioner should be able to take a case to the courts.

c. **Court:** The individual and the privacy commissioner should be able to take a complaint to the district level court, high court, or the Supreme Court of India and seek compensation for the harm caused by the violation.
d. **Remedies:** Any person, who suffers damages caused by non-compliance with the principles or any obligation under the Act, should be entitled to remedy from the data controller to the full extent of the damages suffered. Actors that can be held liable by individuals include data controllers, organization directors, agency directors, and heads of Governmental departments.

Offences, Penalties, and Remedies

7.28. The infringement of any provision under the Act will constitute as an offence by which individuals may seek compensation for, and organizations/bodies held accountable to.

7.29. As found in the UK Data Protection Act, and the Australian Privacy Act the following could be broad offences under the Act:

- **Non-compliance with the privacy principles**
- **Unlawful collection, processing, sharing/disclosure, access, and use of personal data**
- **Obstruction of commissioner**
  - Failure to comply with notification issued by commissioner
  - Processing data after receiving a notification
  - Failure to appear before commissioner
  - Failure to produce documents requested by commissioner
  - Sending report to commissioner with false or misleading information

Annex 1:

Terms of Reference of Group of Experts

F.NO. 13040/47/2011-CIT&I
Planning Commission
(CIT & I Division)

YojanaBhawan, SansadMarg
New Delhi
Dated: 26th December, 2011

OFFICE MEMORANDUM

Subject: **Constitution of Group of experts to deliberate on Privacy issues.**

It has been decided to constitute a Small Group of Experts under the Chairmanship of Justice A.P. Shah, Former Chief Justice, Delhi High Court, to identify the privacy issues and prepare a paper to facilitate authoring the Privacy Bill. The constitution of the group and ToR are as follows:

1. Constitution of the Group:

S. No	NAME & DESIGNATION	
i)	Justice A.P. Shah, Former Chief Justice, Delhi High Court	Chairman
ii)	Shri. R S Sharma, DG UIDAI	Member
iii)	Dr Gulshan Rai, Director General CERT-In, DIT	Member
iv)	Sh. Rajiv Kapoor, JS, DOPT	Member
v)	Representative, Department of Legal Affairs	Member
vi)	Sh. Som Mittal, President, NASSCOM	Member
vii)	Ms. Barkha Dutt, NDTV	Member
viii)	Dr. (Ms) Usha Ramanathan, Researcher & Advocate	Member
ix)	Sh. Pranesh Prakash, Programme Manager, Centre for Internet & Society	Member
x)	Dr. Kamlesh Bajaj, CEO, Data Security Council of India (DSCI)	Member
xi)	Dr. Nagesh Singh, Adviser, Planning Commission	Member
xii)	Sh. R K Gupta, Adviser (CIT&I), Planning Commission	Member

2. Terms of Reference

a. To study the Privacy laws and related bills promulgated by various countries.

b. To make an in-depth analysis of various programmes being implemented by GoI from the point of view of their impact on Privacy.

c. To make specific suggestions for consideration of the DOPT for incorporation in the proposed draft Bill on Privacy.

3. The Chairman may co-opt other Members to the group for their specific inputs.

4. The expenditure towards TA/DA in connection with the meetings of the Group in respect of the official members will be borne by their respective Ministries/Departments. Domestic travel in respect of non-Official Members of the group would be permitted by Air India (economy class) and the expenditure would be met by the Planning Commission.

5. The group will be serviced by the CIT & I Division, Planning Commission.

6. The group shall submit its report by 31st March 2012.

(S Bose)
Under Secretary to the Government of India

To:
The Chairman and all Members of the Group of Experts

Copy forwarded to:
1. PS to Deputy Chairman, Planning Commission
2. PS to MOS (Planning, PA, S&T and ES), Planning Commission
3. PS to all Members of the Planning Commission
4. PS to Member Secretary, Planning Commission
5. Director (PC), IFA unit, Deputy Secretary (Admn.), Planning Commission
6. Administration/Accounts/General Branches, Library, CIT & I Division, Planning Commission
7. Information Officer, Planning Commission

(S Bose)
Under Secretary to the Government of India

Subsequently, Shri R Raghupathi, Additional Secretary, was nominated as a member to represent Department of Legal Affairs. Centre for Internet & Society was represented by Sh Sunil Abraham. Ms. Mala Dutt, Adviser Planning Commission represented Planning Commission in place of Dr Nagesh Singh on his transfer from Planning Commission.

The following members were co-opted to the Group by the Chairman.

Coopted Members		
xiii	Sh. Arghya Sengupta, Oxford University, UK	Member
xiv	Sh. Prashant Reddy, Hyderabad	Member

Annex 2:
How existing privacy protection norms uphold suggested privacy principles

Principle	PUCL	TA[lxxvi]	ITA decrypting[lxxvii]	ITA Monitoring of traffic data[lxxviii]	ISP[lxxix]	UASL
Openness						
Accountability	1. Orders sent for review 2. Specified authority who may require interception 3. Review of legality by committee:	1. Orders sent for review by committee.[lxxx] 2. Specified officer to whom information can be disclosed.[lxxxi] 3. Security Agency Nodal Officers[lxxxii] 4. Service Provider Nodal Officer[lxxxiii] 5. Service providers must acknowledge receipt of request.[lxxxiv] 6. Lists of received orders sent to security agency by service provider[lxxxv]	1. Orders sent for review by committee[lxxxvi] 2. Specified officer to whom information can be disclosed:[lxxxvii] 3. Authorized Agencies Nodal officers[lxxxviii] 4. Intermediary Nodal officer[lxxxix] 5. Service providers must acknowledge receipt of request[xc] 6. Lists of received orders to be sent to security agency by intermediary.[xci]	1. Orders sent for review by committee[xcii] 2. Specified officer to whom information can be disclosed.[xciii] 3. Authorized Agency Nodal officer.[xciv] 4. Intermediary Nodal officer.[xcv] 5. Service providers must acknowledge receipt of request.[xcvi] 6. Lists of received orders to be sent to security agency by intermediary.[xcvii]	1. Compliance with TA[xcviii] 2. Authorizing authorities.[xcix]	1. Compliance with TA.[c] 2. Authorizing authorities.3 Surprise checks by licensor.[ci]
Notice						
Choice & Consent						

Principle	PUCL	TA[lxxvi]	ITA decrypting[lxxvii]	ITA Monitoring of traffic data[lxxviii]	ISP[lxxix]	UASL
Collection Limitation	1. Specific Directions 2. Limitation on duration of interception for two months or extended to six months. 3. Destruction of records as soon as retention is no longer needed.	1. Reasons for interception order[cii] 2. Established conditions for authorisation by competent authority.[ciii] 3. Specific Directions of interception required.[civ] 4. Limitation on duration of interception for sixty days or renewed for 180 days.[cv] 5. Specification of information that may be required to be intercepted[cvi] 6. Destruction of records by security agencies after six months.[cvii] Destruction of records by service providers after two months.[cviii]	1. Reasons for interception order.[cix] 2. Established conditions for authorisation by competent authority.[cx] 3. Specific directions of interception required [cxi] 4. Limitation on duration of interception for not more than sixty days and may not be renewed beyond 180 days.[cxii] 5. Specification of information that may be required to be monitored, intercepted, decrypted etc.[cxiii] 6. Destruction of records by LEA's after six months.[cxiv] Destruction of records by intermediaries after two months.[cxv]	1. Reasons for monitoring or recording order.[cxvi] 2. Established purposes and pre-conditions for monitoring:[cxvii] 3. Specific directions. 4. N/A 5. Specification of Information that may be monitored, recorded, or disclosed.[cxviii] 6. Destruction of records after 9 months from receipt of direction by LEA.[cxix] Destruction within a period of six months by intermediary.[cxx]		
Use Limitation	1. Other means considered before issuing order	1. Other means considered before issuing order.[cxxi]	1. Other means considered before issuing order.[cxxii] 2. Use limited to investigation.[cxxiii]	1. use limited to investigation[cxxiv]		1. Limited to using information only as necessary.[cxxv]
Access & Correction						

Principle	PUCL	TA[lxxvi]	ITA decrypting[lxxvii]	ITA Monitoring of traffic data[lxxviii]	ISP[lxxix]	UASL
Security		1. Service Provider to ensure internal check for security and privacy.[cxxvi] 2. Responsibility and liability of service provider employees.[cxxvii] 3. Unauthorised interception prohibited	1. Intermediary to ensure internal check for security and privacy.[cxxviii] 2. Responsibility and Liability of intermediary employees.[cxxix] 3. Unauthorised interception, monitoring, decryption prohibited.[cxxx] 4. Prohibition of disclosure by intermediary.[cxxxi] 5. Confidentiality over collected material.[cxxxii]	1. Intermediary to ensure internal check for security and privacy[cxxxiii] 2. Responsibility and Liability of intermediary employees.[cxxxiv] 3. Unauthorised monitoring and tracing prohibited.[cxxxv] 4. Prohibition of disclosure by authorized agency.[cxxxvi] 5. Confidentiality over collected material.[cxxxvii]	1. Protection of Privacy of communications by service provider.[cxxxviii] 2. Security required for information transacted over network.[cxxxix]	1. Protection of Privacy of communications by service provider.[cxl] 2. Confidentiality[cxli] 3. Licensor to issue licensee Security clearance[cxlii] 4. Security required for information transacted over network. Information secure.[cxliii]
Disclosure & Third Party Use					1. No transfer or routing of domestic traffic outside of India, especially accounting and subscriber information.[cxlivcxlv]	1. Non-disclosure to third parties unless needed.[cxlvi] 2. No Transfer or routing domestic traffic outside of India, especially accounting and subscriber information.[cxlvii]

Annex 3:
Questions for Analysing Projects / Legislations / Bills from Privacy Perspective

- What personal information is collected by the project and for what purpose?
- Does the agency collect this information directly from the citizens or it is collected by some other agency / third party on behalf of the agency?
- Is the information collected in dispersed locations, or in a central place? Or does the agency collate information from other government sources / agencies?
- Does the agency have a visibility over the personal information collected and associated attributes (e.g. data flows) at the overall project level?
- How does the agency ensure that information which is necessary is collected, and used, only for the specified purposes?
- Does the agency have a privacy policy?
    - If yes, what are its contents (privacy principles)? How is it enforced?
    - Is it compulsory for the citizens to provide information or they have option to not provide information?
    - If citizens choose not to provide information, what are the consequences?
    - Are the citizens informed about the collection of their information, the purpose for which it is collected, etc.?
    - Is their consent taken? If yes, how is it taken and recorded?
    - Is the consent general across time, or is it for the purpose and period specified?
- Do the citizens have access to their information?
    - Can they update it whenever necessary?
- For how long is the information retained?
    - How this period is determined (regulatory requirement, project requirement, etc.)?
    - How is the information deleted after the expiry of retention period?
    - How does the agency ensure that information has been successfully deleted from its own systems and third party systems?
    - Is there a provision for deletion of the data initiated by the data subject?
- In projects where the information is collated from other sources / agencies, are the citizens aware of the same?
    - What is the legal sanctity of doing so (which law / regulation authorizes such collection)? Has individual consent been taken?
    - Do individuals have to be informed when their data is being transferred or shared with another agency?
    - Is it different depending on whether the transfer of the data is to governmental agency?
- Does the project have a Privacy Officer / Security Officer or equivalent who is responsible for protecting privacy?
- What are the organisational, technological and legal measures taken by the agency for securing the personal information? Such measures could include designing and implementation of privacy program, privacy impact assessments, privacy audits, privacy enhancing technologies, etc.
- Are the systems storing personal information exposed to the Internet? If yes, what specific measures have been taken for protection?

- In case of involvement of other agencies / third parties (for collection, processing, etc.), how does the agency ensure protection of personal information by such agencies / third parties (e.g. de-identification, anonymization, contracts, etc.)?
- Especially, what are the safeguards to protect information from resources such as system administrators who have access to servers, databases, etc?
- How is privacy and security factored in the RFPs / contracts?
- How is the 'insider threat' addressed by the agency?
- Who gets to handle the data through the process of collection, storing, use, handling and related transactions?
- Is there any audit and monitoring mechanism for ensuring compliance to privacy policy / validating the measures deployed for privacy protection?
- How is transaction data maintained? For how long?
    - And who can access such transaction data?
- Is the project covered under the IT (Amendment) Act, 2008?
    - If yes, how has the agency ensured that it complies with the ITAA 2008 esp. section 43A?
- Is there any specific law / bill created that has provisions for protecting privacy? If yes, what are the provisions that address privacy?
- How is a privacy breach handled?
- What is the grievance redress mechanism, compensation available to the victims?
- How does the agency ensure that the information collated is not used for 'user profiling' by linking information with other databases using unique identifiers?
- What is the policy on convergence, and on bridging silos of information?
- In case of surveillance / interception related projects, what is the legal process for authorisation?
- What special safeguards such as providing notice, taking consent, etc. are deployed for protection of privacy?
- What are the conditions (such as national security) under which the agency can disclose the personal information to other agencies / third parties (e.g. law enforcement agencies)?
- How does the project ensure that poor and illiterate citizens are smoothly integrated in the technology enabled environment (e.g. awareness about their rights, information access, taking consent, etc.)
- How are actions initiated in the event of identity theft, data theft, and breach of privacy?
- Have there been any actions initiated so far?
- Is the agency collecting sensitive data? What protections are in place in relation to such data?
    - Is the data subject informed about the ways in which the information is to be imparted?
    - Is consent involved in collecting, and storing sensitive data?

Additional question for the health system:

- While digitizing and using health records, how is confidentiality between doctor and patient maintained?

Additional questions for NATGRID

- What are the procedures adopted/proposed for verifying the extent of data that is asked for by the security/intelligence agencies?
- What is the oversight, legislative and privacy regimes that govern the various agencies that NATGRID seeks to facilitate?

ENDNOTES

[i] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation) Available at: http://ec.europa.eu/justice/data-protection / document / review2012 / com_2012_11_en.pdf

[iiii] Id. Article 4 & 7

[iii] Id. Article 18-22

[iv] Id. Article 19(2)

[v] Id. Article 7(1)

[vi] Id. Article 9(1)

[vii] Id. Article 17

[viii] Id. Article 18

[ix] Id. Article 20

[x] Id. Article 22

[xi] Id. Article 30(3)

[xii] Id. Article 30

[xiii] Id. Article 31

[xiv] Id. Article 33

[xv] Id. Article 35(1)(b)

[xvi] Id. Article 38(2)

[xvii] Id. Article 39

[xviii] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[xix] Id. Principle 1

[xx] Id. Principle 2

[xxi] Id. Principle 3

[xxii] Id. Principle 4

[xxiii] Id. Principle 5

[xxiv] Id. Principle 6

[xxv] Id. Principle 7

[xxvi] OECD Privacy Principle. Available at: http://oecdprivacy.org/

[xxvii] APEC Privacy Framework. Available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

[xxviii] For Your Information: Australian Privacy Law and Practice (ALRC Report 108). Available at: http://www.alrc.gov.au/publications/report-108

[xxix]The Exposure Draft is available at: http://www.smos.gov.au/media/2010/docs/Privacy-reform-exp-draft-part-1.pdf (last visited 23 April 2012); A Companion Guide to these Principles is also available on file with the author.

[xxx] For a succinct analysis of the 13 APPs, see Norman Witzleb, Exposure Draft of the New Australian Privacy Principles- The First Stage of Reforms to the Privacy Act 1988' 39 *Australian Business Law Review* 58 (2011).

[xxxi] The Ontario Supreme Court has held recently that a tort of intrusion upon seclusion exists in Johnson v. Tsige available at http://canlii.ca/en/on/onca/doc/2012/2012onca32/2012onca32.html (Last visited 23 April, 2012).

[xxxii] RSC, 1985, c P-21.

[xxxiii] S.C. 2000, c. 5.

[xxxiv] Note that the regulation of privacy in Canada is also influenced by Ontario's Information and Privacy Commisioner's Principles of "Privacy by Design (PbD)". *See* http://privacybydesign.ca/about/principles/ (Last visited 23 April, 2012).

[xxxv] Personal Information Protection and Electronic Documents Act 2000. Available at: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[xxxvi] Id. s. 2 (1)

[xxxvii] Id. s. 4 (2)

[xxxviii] Id. s. 2.1

[xxxix]Id. s. 4.1 Principle 1

[xl] Id. s. 4.2 Principle 2

[xli] Id. s. 4.3 Principle 3

[xlii] Id. s. 4.4 Principle 4

[xliii] Id. s. 4.5 Principle 5

[xliv] Id. s.4.6 Principle 6

[xlv] Id. s. 4.7 Principle 7

[xlvi] Id. s.4.8 Principle 8

[xlvii] Id. s.4.9 Principle 9

[xlviii] Id. s.4.10 Principle 10

[xlix] The Privacy Act 1985 available at: http://laws-lois.justice.gc.ca/eng/acts/P-21/index.html

[l] Id. s.2

[li] Id. s 3& s.71

[lii] Id. s.5

[liii] Id. s.4

[liv] Id s.7

[lv] Id. s. 6(2)

[lvi] Id. s.11

[lvii] Id. s. 10

[lviii] Id. s. 12, 13, 14

[lix] Id. s.29&30

[lx]Right to Information Act, 2005, s.18

[lxi] Human DNA Profiling Bill 2012. Available at: http://bargad.files.wordpress.com/2012/06/1draft-human-dna-profiling-bill-2012.pdf

[lxii] The Citizenship Act 1955 Available at: http://mha.nic.in/pdfs/ic_act55.pdf

Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003: Available at: http://censusindia.gov.in/2011-Documents/citizenship_rules2003.pdf

[lxiii] The Collection of Statistics Act 2008 Available at: http://mospi.nic.in/mospi_new/upload/COS_Act_2008_English_26may11.pdf?status=1&menu_id=159

The Collection Statistics Rules 2011 Available at: http://mospi.nic.in/Mospi_New/site/inner.aspx?status=3&menu_id=173

[lxiv] The Unique Identification Bill 2010. Available at: http://164.100.24.219/BillsTexts/RSBillTexts/asintroduced/national%20ident.pdf

[lxv] ITA Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011. Available at: http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511%281%29.pdf

[lxvi] As practiced in the UK RIP Act. s.57. Available at: http://www.legislation.gov.uk/ukpga/2000/23/section/57

[lxvii] As practiced in the US Wiretap Act. Available at: http://www.ncsl.org/issues-research/telecom/electronic-surveillance-laws.aspx

[lxviii] As practiced in the UK RIPA Act. S.19 Available at :http://www.legislation.gov.uk/ukpga/2000/23/section/19

[lxix] These are drawn from the UK CCTV code of practice available at http://www.ico.gov.uk/upload/documents/cctv_code_of_practice_html/9_responsibilities.html

[lxx] The Indian Express (2012). Gang rape effect: Don't let women work beyond 8pm in pubs, mall. Available at: http://www.indianexpress.com/news/gangrape-effect-dont-let-women-work-beyond-8-pm-in-pubs-malls/923453/0. Last accessed: August 22nd 2012.

[lxxi] Vyas, S. Committee sets new terms for CCTV tenders. Times of India August 22nd 2012. Available at: http://articles.timesofindia.indiatimes.com/2012-08-22/mumbai/33321643_1_security-cameras-mla-funds-cctvs. Last Accessed: August 31st 2012.

[lxxii] Uppar. R. CCTV cameras to ward off baby stealers. Times of India. August 22nd 2012. Available at: http://articles.timesofindia.indiatimes.com/2012-08-22/hubli/33322003_1_cctv-cameras-maternity-ward-expectant-mothers. Last accessed: August 29th 2012.

[lxxiii] Best practices provided by GeneWatch UK and Council for Responsible Genetics in the "Overview and concerns regarding the Indian Draft DNA Profiling Act" available at: http://cis-india.org/internet-governance/indian-draft-dna-profiling-act

[lxxiv] Devulapalli, R. Doubting parents can buy 'peace' for Rs.10K. Times of India. August 29th 2012. Available at: http://articles.timesofindia.indiatimes.com/2012-08-29/hyderabad/33475385_1_dna-test-dna-sample-g-v-rao. Last Accessed. August 30th 2012.

[lxxv] Business Standard. Female DNA found on Aarushi's parents' clothes: Forensic expert. Business Standard. September 1st 2012. Available at: http://www.business-standard.com/generalnews/news/female-dna-foundaarushis-parents-clothesforensic-expert/44275/. Last Accessed: August 30th 2012.

[lxxvi] Rule 419-A of the Indian Telegraph Rules, as amended by the Indian Telegraph (Amendment) Rules, 2007

[lxxvii] Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

[lxxviii] Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

[lxxix] Internet Service Provider License Available at:

lxxx. Id. Rule 419-A (2)

lxxxi. Id., Rule 419-A (16), (5)

lxxxii. Id., Rule 419-A (16), (9)

lxxxiii. Id., Rule 419-A (16), (10).

lxxxiv. Id., Rule 419-A (16), (11).

lxxxv. Id., Rule 419-A (16), (13).

lxxxvi. Rule 7. Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

lxxxvii. Id. Rule 10

lxxxviii. Id. Rule 12

lxxxix. Id. Rule 14

xc. Id. Rule 15

xci. Id. Rule 18,

xcii. Rule 7.Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

xciii. Id. Rule 4.3

xciv.Id. Rule 4.2

xcv.Id. Rule 4.4

xcvi. Id. Rule 4.8

xcvii.Id. Rule 4.10

xcviii. Clause 35.1 ISP License

xcix.Id. Clause 34.28 (xix).

c.Id. Clause 41.19(vi) (xix).

ci. Clause 41.9 (iii) UASL License

cii. Rule 419-A (16), (2)

ciii. Section 5(2), Telegraph Act, 1885.

civ. Rule 419-A (16), (4)

cv. Rule 419-A (16), (6)

cvi. Section 5(2), Telegraph Act, 1885.

cvii. Rule 419-A (16), (18).

cviii. Rule 419-A (16), (19).

cix. Rules 7 Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

cx. Section 69, Information Technology Act, 2000.

cxi. Rules 9 Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

cxii. Id. Rule 11

cxiii. Id. Rule 9

cxiv. Id. Rules 23

cxv. Id.

cxvi. Rule 3.3 Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

cxvii. Id. Rule 3

cxviii. Explanation (ii), Section 69B, Information Technology Act, 2000 (as amended).

cxix. Rule 8.1 Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

cxx. Id. Rule 8.2

cxxi. Rule 419-A (16), (3)

cxxii. Rules 8, Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

cxxiii. Id. Rule 25.2

cxxiv. Rule 9. 4. Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

cxxv. UASL clause 39.2 (a)

cxxvi. Rule 419-A (16), (14).

cxxvii. Rule 419-A (16), (15)

cxxviii. Rules 20, Information Technology (Procedure and Safeguards for Interception and Decryption of Information) Rules, 2009

cxxix. Id. Rules 21

cxxx. Id. Rules 24

cxxxi. Id. Rule 25

cxxxii. Id. Rule 25.4

cxxxiii. Rule 5 Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information)

cxxxiv.Id. Rule 6

cxxxv. Id. Rule 9

cxxxvi. Id. Rule 10

cxxxvii. Id. Rule 11

cxxxviii. Clause 8.4, 32.2.*ISP license*

cxxxix. Clause 34..28 (iv) ISP license

cxl. Clause 39 & 41.4. *UASL*

cxli. Clause 39.3UASL

cxlii. Clause 41.6UASL

cxliii. Clause 41.20 (iv) UASL

cxliv. Clause 34.28 (iii) ISP license

cxlv. Clause 34.28 (viii) ISP license

cxlvi. Clause 39.2 (a)UASL License

cxlvii. Clause 41.20 (iii) UASL License