APPROACH PAPER FOR A LEGISLATION ON PRIVACY

A group of officers was constituted to develop a conceptual framework that could serve the country's balance of interests and concern on privacy, data protection and security and which also responds domain legislation on the subject. The group held several meetings and also held discussions with stakeholders groups (civil society organizations, local practitioners, business and banking representatives). Subsequent to these discussions, Shri Rahul Matthan of Tri Legal Services who has been an active participants in these discussions has prepared an approach paper for the legal framework for proposed legislation on privacy. The approach paper, with some modifications including some suggestions made by Shri Kamlesh Bajaj, CEO, Data Security Council of India is now being circulated for seeking opinions of the group of officers and is also being placed on the website of the Department of Personnel and Training for seeking public views on the subject.

What is Privacy?

Privacy for the purpose of this approach paper could particularly be defined as the expectation that confidential personal information disclosed by any individual to Government or non-Government entity should not be disclosed to third parties without consent of the person and sufficient safeguards need to be adopted while processing and storing such information. In essence, disclosure of data which can be used to identify a physical person without following the due procedure could be construed as breach of privacy.

Is there a need for privacy protection?

India does not currently have a general data protection statute. Nevertheless, the judiciary has derived a "right of privacy" from the rights available under Articles 19(1)(a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution of India. However, all cases that deal with the right to privacy have been decided in the context of Government actions that resulted in private citizens being denied their right to personal privacy. No privacy judgment has granted private citizens a right of action against the breach of privacy by another private citizen. To that extent, the data protection and personal privacy jurisprudence in the country is not yet fully developed.

India is not a particularly private nation. Personal information is often shared freely and without thinking twice. Public life is organized without much thought to safeguarding personal data. In fact, the public dissemination of personal information has over time, become a way of demonstrating the transparent functioning of the government. While many agencies of the government collect personal data, this information is stored in silos with each agency of the government maintaining information using different fields and formats. Government databases do not talk to each other and given how differently they are organized, the information collected by different departments cannot be aggregated or unified.

Data privacy and the need to protect personal information is almost never a concern when data is stored in a decentralized manner. Data that is maintained in silos is largely useless outside that silo and consequently has a low likelihood of causing any damage. However, all this is likely to change with the implementation of the UID Project. One of the inevitable consequences of the UID Project will be that the UID Number will unify multiple databases. As more and more agencies of the government sign on to the UID Project, the UID Number will become the common thread that links all those databases together. Over time, private enterprise could also adopt the UID Number as an identifier for the purposes of the delivery of their services or even for enrollment as a customer. Once this happens, the separation of data that currently exists between multiple databases will vanish.

Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data before the vast government storehouses of private data are linked up and the threat of data security breach becomes real.

Similarly, the private sector entities such as banks, telecom companies, hospitals etc are collecting vast amount of private or personal information about individuals. There is tremendous scope for both commercial exploitation of this

information without the consent/ knowledge of the individual consent and also for embarrassing an individual whose personal particulars can be made public by any of these private entities. The IT Act does provide some safeguards against disclosure of data / information stored electronically, but there is no legislation for protecting the privacy of individuals for all information that may be available with private entities.

In view of the above, privacy of individual is to be protected both with reference to the actions of Government as well as private sector entities.

3.Is there a need for such legislation?

Notwithstanding the concerns around the risks posed by this vast interconnected public information database, there are issues being raised about the need to even have a legislation in the first place. The argument being made is that given the technical and highly dynamic nature of personal data, a heavy legislative approach is probably unwarranted. Instead, industry self-certification could achieve the same results without the downsides of putting in place a legislative and regulatory framework.

In order to implement this, various industry verticals would need to appoint independent certifying agencies to prescribe data standards and to overlook compliance with data protection principles. The system is voluntary but relies on peer pressure to ensure that conscientious corporations remain compliant with their obligations in order to continue to be accepted by their customers and business ecosystem.

While this suggestion does offer a lighter touch, it does not give the individuals, whose data is at risk, any form of legal remedy in case of a breach of their personal privacy by the self certifying organizations. In the event any such organization commits a data breach, the individual whose data has been lost will have no legal recourse. Data protection can only be ensured under a formal legal system that prescribes the rights of the individuals and the remedies available against the organization that breaches these rights. It is imperative, if the aim is to create a regime where data is protected in this country, that a clear legislation is drafted that spells out the nature of the rights available to individuals and the consequences that an organization will suffer if it breaches these rights.

It is possible to develop a hybrid approach where a statute is enacted to provide the contours within which all organizations, private and public, are to conduct themselves with regard to personal information that they collect. Industry associations could then define more detailed guidelines and practices that member organizations would need to follow with specific reference to the specific issues of that industry.

4.**Legislative competence**

Before embarking on the exercise to prepare a data protection legislation, it is important to ascertain whether the Centre has the legislative competence to enact such a law. Article 246(1) of the Constitution of India grants the Parliament the power to legislate on matters set out in List I of the Seventh Schedule of the Constitution. This list does not specifically contain an entry under which data protection laws may be classified. However, entry 97 provides the Parliament with the authority to legislate on any matter not enumerated in List II of the Seventh Schedule (the State List) and List III of the Seventh Schedule (the Concurrent List). In the absence of specific data protection entries in the other lists, it would appear that entry 97 grants the Parliament the residuary powers needed in order to make laws on any matters it deems fit in national interest, including the power to enact the data protection legislation.

5.**Is there is constitutional right to Privacy?**

In certain countries, such as South Africa and Argentina, the right to privacy is incorporated into the constitution. In India, the right of privacy has been derived through judicial decisions, from the rights available under Articles 19(1) (a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution. There was no specific discussion on the concept of privacy in the Constituent Assembly Debates. However, over time, the Supreme Court has held that even though the right to privacy is not expressly enumerated as a fundamental right, it could certainly be inferred from the fundamental rights guaranteed under the Constitution.

Article 19(1)(a) states that -

All citizens shall have the right to freedom of speech and expression.

The Supreme Court has, through a series of decisions held that, even though the right to privacy was not enumerated as a fundamental right, it could certainly be inferred from the fundamental rights of the Constitution. However, these fundamental rights are not without restrictions. Just as Article 19(1)(a) bestows on each citizen the fundamental right of freedom of speech and expression, Article 19(2) imposes restrictions on this right. It states that:

Nothing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, 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 offence.

The necessary implication of this is that the Government can deprive a citizen of his constitutional right of freedom of speech and expression for any of the reasons set out in Article 19(2). By natural extension of this principle, the Supreme Court, in Gobind v. State of Madhya Pradesh, held that a violation of personal privacy is possible with the sanction of law.

However this position was clarified and extended in People's Union of Civil Liberties v. the Union of India where the right of government authorities to intercept, in the interests of national sovereignty, messages transmitted or received by any telegraph, was challenged in the context of

wire tapping. The Supreme Court held that tapping a person's telephone line violated his right to privacy, unless it was required in the gravest of grave circumstances such as in the case of a public emergency. This case was significant in that while the court upheld the restrictions on the fundamental freedoms that have been guaranteed under the constitution, it insisted that the government must use restraint in exercising these powers.

All available cases on this point have been decided in the context of government actions that resulted in the deprivation of personal privacy of individuals. There has been no case decided in the context of the infringement of personal privacy by private citizens. It is therefore unclear as to how these precedents will apply in such cases.

6.**Existing legislations**

There is not data protection statute in the country. However, the Information Technology Act, 2000 (the "**IT Act**") contains provisions under which certain Government agencies can gain access to data. The IT Act was recently amended and two new sections, 43-A and 72-A, were inserted dealing with data protection.

Section 43-A prescribes compensation in the event a body corporate that possesses, deals or handles any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and consequently causes wrongful loss or wrongful gain to any person. This section makes no mention of non-digital data. A data protection legislation should cover within its ambit data stored in any electronic medium or a relevant filing system (such as a salesperson's diary). This section does not provide any protection to data stored in the non-electronic medium. In addition, though the section does make mention of sensitive personal information it does not do so in comparison with personal information which is at a very different level. In essence, under this provision there appears to be no difference between what is traditionally considered to be personal information and sensitive personal information.

Section 72-A prescribes punishment for disclosure of information in breach of a lawful contract. Any person who, in the course of providing services under a lawful contract, gains access to any material containing personal information discloses, without consent, or in breach of the contract, this material to anyone else will be punished. The problem with this provision is that there is no definition of personal information and in the context of the provisions of Section 43-A that speaks of personal sensitive information, creates a bit of inherent confusion between different sections of the IT Act. While the section does criminalise the act of breach of confidentiality, it does not offer any form of compensation to the victims of such breach. In the context of invasion of privacy, that is probably the most important remedy. The section is narrowly drafted and only deals with personal information obtained under the provisions of a contract for providing services. As a matter of fact, personal information can be obtained through a number of different methods and all such personal information must be protected.

While these amendments do provide some amount of protection against breaches of privacy they are in no way a complete solution. It is important that terms such as "personal information" and "sensitive personal information" are defined clearly. A higher degree of care must prescribed for, sensitive personal information, in terms of its collection, utilization and disclosure. It is also important to ensure that data stored in the non-electronic medium should also be covered and protected. More importantly, while the provisions newly introduced into the IT Act 2008 provide a framework for data protection into the country, where none existed before, a full fledged data protection legislation needs to include regulations on collection, control, utilization and proper disposal of data. These important principles must be addressed to have an effective data protection regime in India.

7.**Potential Conflicts between Data Protection legislation and other Laws**

There have been various concerns voiced about the fact that the enactment of a data protection regime will conflict with some already existing and necessary legislations. In this regard questions have been raised about data protection in the context of the right to information as well as in the context of credit verification processes. Can a data protection law co-exist with these statutes?

7.1 Data Protection and the Right to Information

There are some concerns about whether the rights granted by a privacy legislation would run contrary to the rights available under the Right to Information Act which provides citizens the right to access public information.

In the first place, data protection legislations exist around the world even in countries that have enacted detailed public information access legislations. These two types of laws have been proven to be capable of existing side by side. It could even be said that the right to protect private data sits at the other end of the spectrum from the right to access public data. Rather than being contradictory, they operate antipodally from each other and give each other meaning.

The right to information under the RTI Act relates to such information as is available with a public officials including work, documents, records, sample of information etc. which a citizen has a right to access. This, in itself, is the inbuilt protection available for personal information. Thus, just as an individual has the right to access public information, he has the right to prevent unauthorized access to his personal information. In fact, there are several provisions in the RTI Act which directly or indirectly reinforce that private information relating to an individual is to be prevented from unauthorized disclosure. For example, Section 11 prescribes that information relating to or supplied by a third party which has been treated as confidential by the third party can not be disclosed without his / her consent. Similarly Sub sections 8(1) (d), 8(1)(e) and 8 (1)(j) exempts disclosure of personal information in various circumstances. As such, a well defined data protection regime will be synergistic to the provisions of the RTI Act.

However, despite the existence of a specific exemption under Section 8 of the RTI Act, there is still no clarity as to whether the personal data of public officials falls within the exemption. Under the RTI Act, it might be possible for citizens to claim a public interest in accessing personal information of such public servants and given that the law does not make this clear, could use this provision to invade the personal privacy of a government servant. It may be advisable to consider special provisions to address this lacuna in the proposed data protection legislation.

7.2 Data Protection and Credit Verification

Credit verification is the bedrock upon which modern banking systems are based. In that context, banks and financial institutions rely upon the ability to access personal information about prospective borrowers in order to be able to assess whether or not they should be granted a loan. Once a data protection legislation is passed would this result in a curtailment of this right and consequently would this have a detrimental effect on the banking system?

Data protection statutes do not bar the collection of data. They merely regulate the manner in which data is collected and processed. Most data protection legislations limit the processing of the personal information for the purpose for which it was collected. Accordingly, so long as personal information provided for verifying the credit-worthiness of a person is used for that purpose alone, there would be no problem using such information under the proposed data protection legislation.

Additional requirements could be imposed on the processing of such data. For instance the UK Data Protection Act has specific provisions dealing with situations where the data controller is a credit reference agency. The data protection law in Denmark lays down specific instances when data about debts to public authorities can be disclosed to credit information agencies. The act states explicitly that such confidential information will not be disclosed to the general public. In

Austria, applications to check information relating to the creditworthiness of an individual can only be initiated after examination by the Data Protection Commission.

7.3 Data Protection and Private Investigative Agencies

There is a further potential conflict between the business of private surveillance and investigation and personal data protection. Would the enactment of a data protection law result in the curtailment of the freedom to trade of detective agencies?

A number of European countries have specific enactments dealing with the use of surveillance for security and private investigation purpose and the review of information obtained. Private investigators have to be licensed in many countries. In Ireland, it is necessary that physical and electronic surveillance measures must comply with data protection laws.

Given that private detective agencies, if allowed to operate without regulation, could potentially wreak considerable havoc on the personal information of a citizen, it is important to ensure that these agencies are regulated particularly when it comes to the use of personal information. The introduction of a data protection legislation, could have significant consequences on this industry.

7.4 Data Protection and National Security

There is likely conflict between privacy needs of an individual and interests of national security. On many occasions Government may need to resort to gaining access to personal information and its sharing with other government agencies in order to safeguard national interests. Privacy legislation will need to provide for such exceptions.

7.5 Data Protection Vs. Transparency in Government

In recent times, the government has, in order to demonstrate greater transparency in its functioning and reduce corruption, initiated the practice of publishing complete details of all the government activities with full information about the recipients of government service. While these initiatives do go a long way to validate the fact that government servants have honestly and without fraud or corruption, delivered the services they are obliged to provide, they have the unintended consequence of exposing vast quantities of personal data in a very public way. With the introduction of the UID number this practice could result in even greater harm as the UID number that will be present in each and every publication of this nature will make it easy to link various public databases and help create an identifiable profile of everyone on that public database.

The government needs to balance the need for transparency with the social obligation to provide its citizens with personal privacy and data protection. There are other ways in which transparency could be demonstrated – ways that do not impinge upon personal privacy. In enacting a data protection legislation, the government should be making a policy decision that it supports personal privacy and if this means re-thinking its approach to transparency, must be willing to take appropriate measures to change its own thinking.

8.0 Privacy Legislations in other countries

Many countries in Europe, Asia and America have enacted privacy legislations. A summary of the key provisions of legislations of major countries is Annexed. A perusal of the summary would suggest that approach to protection of privacy and individual liberty adopted by the various countries have many common features. It is possible to identify certain basic values which are commonly considered to be elementary components of the area of protection. Some of these principles are setting limits of the collection of personal data in accordance with the objectives of the data collector and similar criteria; restructuring the usage of data to conform with specific purposes, granting facilities for individuals to know all the exceptions and constraints of data and

have their data collected; and the identification of parties who are responsible for compliance with the relevant privacy protection of rules and decisions.

Differences between approaches of various countries referred to aspects such as the scope of legislation, the emphasis placed different elements of protection, exceptions provided in the law, and the machinery of enforcement. While most of the European legislations have opted for heavy handed enforcement, many of the countries in South East Asia have preferred the light handed self-regulator. However, as noted above, the core principles are by and large common amongst the countries and as described in legislature, some of the common principles for privacy legislations may be enumerated below:
Notice
Choice and Consent: Consent of the individual before his personal information is collected and maintained.
Collection Limitation : only that information is to be collected that is essential for the purpose.
Use Limitation : Information is to be strictly used for the purpose for which it was collected.
Access and Correction : an individual should be allowed access to his information and he should be enabled to correct / update his information.
Security : data is to be secured against accidental loss or theft.
Disclosure to third party : Individual's consent is required for disclosure of his personal information to third parties.
Openness : the data controller would be transparent in his working as regards the collection and use of personal data.
Accountability : of the data controller and his agents for safety of personal data, its use and its
Preventing Harm: to the individual whose personal information is being stored by the private or government entity.

It is recommended that these principles be adopted for the proposed framework also.

9.0**Proposed Framework for Privacy Legislation**

Based on the above a framework is being outlined in subsequent paras. The key recommendation is that the legislation should really be in the form of framework rather than detailed prescriptions. It should highlight the basic principles that any data controlling authority will need to subscribe to and how the privacy rights of an individual would be protected. Thereafter the sector-specific or industry specific detailed guidelines will be prepared and approved by the regulator which wouild also be responsible for enforcing the legislation. The specified features of the framework are discussed below in detail:

9.1**Applicability**

Almost all data protection legislations have a well defined applicability clause, determining the persons who have to comply with the obligations set out therein. Of the statutes examined, 5% are applicable only to public bodies and 3% are applicable only to private persons. An overwhelming majority (92%) of the countries reviewed have made their enactments applicable to both public and private entities. Most legislations exclude from the ambit of the legislation, information that is solely in the domestic or household sphere and for strictly personal reasons.

Recommendation

It is strongly recommended that the proposed data protection legislation apply equally to private as well as public entities.

At present, India has a privacy jurisprudence that has been judicially derived from the fundamental rights set out in the Constitution. Through a series of cases the courts have upheld an implicit right against police action that impinges upon the personal privacy of citizens.

However, most of these cases have been argued in the context of invasion of physical privacy and relate to the right of individuals against harassment by governmental authorities.

With the increasing digitization of data, many entities both public as well as private, have collected and currently hold vast amounts of personal data. It is possible that public entities and governmental agencies currently hold much more personal information about a larger section of society than any private entity. There is currently no legislation that protects against the misuse of this data. Should a legislation be passed that addresses the privacy concerns around such data, it is imperative that such a legislation apply equally to public as well as private entities in order to equally protect citizens and individuals against the misuse of their personal data.

9.2**Data**

All the legislations that were examined, with the exception of 13 countries, made a distinction between personal data and personal sensitive data, applying a greater standard of care when dealing with personal sensitive data as opposed to personal data.

Recommendation

In the Indian context, it is advisable that such a distinction be brought about in order to ensure that all forms of identifiable data are protected under the general right to privacy but that a greater responsibility is imposed on entities processing or collecting certain categories of information which if disclosed could result in significant financial, reputational or other associated loss to the person concerned. At present the Information Technology Act, 2000 includes data protection provisions that apply to personal sensitive data alone without making the distinction between that and personal data. It will be important to re-examine the definition as it currently stands in that Act, and suggest an appropriate definition that realistically distinguishes between personal data that deserves some amount of protection and personal sensitive data that requires a greater degree of protection.

9.3**Personal Data**

Almost all the legislations define personal data to mean any information that relates to an identifiable person. Unless the sum total of the information in question has the ability to identify a real person it will not be elevated to the status of personal data.

In most cases, personal data refers to identity information about natural persons. However, some jurisdictions include within the ambit of personal data, identity information about legal persons, bodies or associations.

Recommendation

In the Indian context it is advisable to limit the legislation to personal information relating to real persons as there are other legislations that deal with information in the context of legal persons such as corporations. Besides, there is a greater risk of personal injury in the context of real persons as opposed to legal persons.

It is also important to draw from the best practices of countries around the world in coming up with an appropriate definition for personal data that results in information that is capable of identifying a person, either directly or indirectly (and thereby causing risk to his identity), being included within the ambit of the definition. It is possible that a person could be identified directly by name or indirectly by his car registration number or passport number. It is important to include both types of data within the definition. Equally, it is important to recognize that in all cases a persons name may not be enough to identify him. For instance, "Singh" is a very common family name and may not of itself constitute information that is capable of identifying a person.

It is important to note that to be able to identify a person, information need not necessarily be objective identification such as a person's name, but can be subjective information such as the opinion that a person is a "reliable" borrower or that a person is "expected to die of a terminal disease". It is also important to bring all personal information within this definition regardless of the format in which the information is stored. For instance, video surveillance footage that identifies a person should be classified as personal data in order to protect the privacy of the person involved. Drawings made by patients as part of psychiatric evaluations should similarly be treated as personal information as they could identify the medical condition of the person.

9.4**Personal Sensitive Data**

Definition of personal data is very wide while compared to personal sensitive data, which is more specific and includes various types of information, which, if disclosed inappropriately, could result in financial and reputational loss to the person concerned.

Almost all the legislations examined listed the following as personal sensitive information:

racial or ethnic origin;
political affiliations or opinions;
religious affiliations and beliefs or other beliefs of a similar nature;
membership of a trade union;
physical or mental health or condition;
sexual life; and
criminal record.

In addition, the following categories of information have also been treated as personal sensitive information in some jurisdictions.

Genetic information about an individual that is not otherwise health information;
Information or an opinion about an individual;
Financial or proprietary confidential corporate data;
Data on a person's personality;
Private family relations;
Biometric data;
Social welfare needs of a person or the benefits, support or other social welfare assistance received by the person; and
Data collected on a person during the process of taxation (except data concerning tax arrears).

Recommendations

It is important that an appropriate list of items that would constitute sensitive information in the Indian context be developed. While the first list set out above must form the basis for any list of sensitive information that is to form part of the Indian legislation, it is important that additional elements as appropriate for India be added. For instance, in addition to the reference to racial or ethnic origin in the Indian context special reference must be made to caste as well. Also, in the context of the Aadhar program, it will be relevant to include biometric data in the definition of personal sensitive data. The Group of officers would need to deliberate on this and finalise the definition of personal data and personal sensitive data as this would be one of the key elements of the proposed privacy legislation.

9.5**Data Collection**

All data protection legislations include provisions that deal with and regulate the collection of data. These provisions usually include the following elements:

It is necessary to inform the data subject of the purpose of the collection of data.
The explicit or written consent of the data subject must be obtained for the collection of data. However, the balance of interests must always be considered and in certain cases, the requirement to obtain consent may be dispensed with for reasons such as national security, benefit of the data subject or investigation of a crime or other circumstances that may be prescribed in the statute
The data subject is free to withdraw consent in certain cases.
The data that is collected must only be for specific, explicitly defined and legitimate purposes. For instance, the collection must be authorised under a law. The data subject must consent (such consent being subject to the test of "balance of interests") to his personal data being used for the specified purposes.
Collection of data which is of a sensitive nature is generally subject to more control or may be prohibited. Explicit consent or even approval from a regulatory authority may be required to be obtained to collect sensitive personal data.
Data collected must be proportional to the purpose for which it was collected.
The information that is collected must be accurate and up to date.
Where the information is not received directly from the data subject, the source of the information must be informed to data controller.

Recommendations

Informed written consent should, where supported by the balance of interests, be a necessary prerequisite for collection of data from individuals. The need for written consent in local language or a language known to the subject must be examined. It will also be important to address concerns of illiteracy and the need to ensure that all persons who provide personal data understand why they are doing so and what the data is going to be used for. Informed consent is particularly important where information is being sought from people who do not have the ability to read and write and therefore to understand why the information is being sought. However it is important to recognize that in certain circumstances, such as in relation to the use by employers of personal information of their employees, customers, suppliers and shareholders in the conduct of their business, consent may not be necessary in all instances. Additional exceptions such as collection of data for investigation of criminal offence, national security, health, census etc. may be built in. However, these exceptions must be carefully chosen and narrowly worded to avoid misuse through expansive definition. An exception may need to be made in case of data which government agency collects and an individual is statutorily require to provide such as data for Census.

Data subjects should also be allowed to withdraw consent for data collection even after the data has been collected. The right to withdraw consent is integral to any right to personal privacy. The ability to collect data must come with an obligation to ensure that whenever a data subject wants to be removed from the database, such data subject should have the right to leave.

Data should be collected only for a specific stated purpose. Data once collected must only be used for the purpose for which it was collected. If a data controller is allowed to indiscriminately use the data collected, it would vitiate the informed consent obtained prior to collection. If the data is to be re-used for a different purpose the data subject should have a justiciable right against the data controller for allowing the data so collected to be used otherwise than for the purpose for which it was intended. Implicit in this provision is the obligation on the data controller to only collect that amount of data as is necessary for the stated purpose and no more. While it is true that the proposed data protection legislation will impose restrictions on the collection and use of data, it is in the interests of the general public that this restriction is imposed. Under Article 19(6) of the Constitution, reasonable restrictions can be imposed on the freedom to trade. The data protection legislation has to be read such that it will not impose unreasonable restrictions on the

freedom to trade.

Sensitive personal data must be treated differently from regular personal data. At present no Indian legislation makes this distinction and it is imperative that the country's data protection legislation creates these categories to ensure that some forms of personal data are treated more specially than others.

9.6**Data Processing**

All the legislations we reviewed include regulations with regard to data processing. Since most data leakage takes place during remote processing, is important to ensure that adequate measures are in place to ensure that data transferred to a processor receives the same level of protection. Most data protections legislations include the following provisions with regard to data processing:

The data controller has to ensure that the data processor processes the information/personal data for the purpose for which it was collected.
Data processing must be done carefully and in a diligent manner.
Data processing must for reasonable and legitimate purposes and must be in good faith and in consideration of the interests of the individual.
Data subject must have the knowledge of the purpose for which the data is being processed.
Some countries require that the data in the database is used only for the purposes for which the data base was setup. Also requires the database to be registered subject to certain conditions.
Processing of data in an automated manner must be avoided when it affects the vital interests of the data subject. In some countries the subjects have the right to have knowledge of the logic of the automated processing and in others they may request the same to be supervised by a person.
Processing in a manner that provides unauthorised access of the data to persons other than the data subject is strictly prohibited.

Recommendations

Since the data controller has obtained consent from the data subject for the collection of data it should be the responsibility of the data controller to ensure that any processing that takes place by a third party processor is done with the same standards of data protection required of the data controller. **The data controller must be responsible for the faults of the data processor and should be primarily responsible for compliance by the data processor with data protection obligations.**

It is important that, in the event the data collected needs to be processed, the data subject is informed that it is going to be processed as well as why. Under various circumstances, digital data is processed automatically using computer algorithms. Many data protection legislations include specific provisions that allow data subjects to question such automated decisions. However, considering the population of India, the practical nuances involved in prohibiting the automated process must be considered.

It is important that the individuals be informed of the reasons for which the data will be processed. The data processing must be proportional to the purpose for which it was collected and must be conducted in a diligent manner to avoid any disclosure or unauthorised access.

9.7**Data Storage**

Data once collected needs to be stored and as larger volumes of data enter into public and private databases, the need to legislate on appropriate storage regulations becomes important. No matter how carefully regulated collection and processing might be, if data retention and storage regulations do not match up, there is a grave risk that this will prove to be the source of

data violations. Most legislations around the world have regulations relating to the retention and storage of data. These include provisions such as:

The data once collected must be deleted after achieving the purpose for which it was collected.
Data must not be stored in a form that allows data subject to be identified after achieving the purpose of collection.
Uniform personal identification numbers must not be used for identification of data subjects.
Some countries have prohibited linking of data and use of matching programs.
Laws of some countries mandate that data must be retained for a period after the use so that it can be accessed by the data subjects or by the state.
Some of the exceptions for deletion of data include keeping data for historical, scientific and statistical or research purposes.
The details of data collected to be published in register or in a website.
Access to the data must be blocked if the data cannot be deleted.
The data controller must limit the time period of the retention of information to the minimum necessary.
The details of the time and date when the information is collected for storage must be noted.
Data subjects must be provided with a mechanism to withdraw the consent at any time, without undue delay, cost or gain to the data controller.

Recommendations

It is important to ensure that the data is stored only till the time the purpose for which it was collected is achieved, unless the purpose is for archival purposes, national security purposes etc. Once the purpose has been achieved, the legislation should prescribe that the data so collected should be deleted permanently. Various legislations have suggested lesser levels of protection than deletion (including storing the data in a manner that would not allow the data subject to be identified after the purpose for which it was collected has been achieved), however none of this will be adequate safeguard against the leakage of data that is being stored past its expiry date.

It is also important to prevent the linking of databases. There are many merits to such linkages, particularly in the current social and economic circumstances of India. However, the possibility of misuse exists and the consequences of misuse could far exceed the good that this might bring. If linkage is to be permitted adequate safeguards must be taken to ensure that such linkage does not result in invasion of personal privacy. Obligations to anonymise data or to otherwise protect data subjects from unlawful abuse of their information across databases should be included.

9.8**Data Security**

The data once collected, will need to be stored (even if only for a little while), by the data controller. It is important that the proposed data protection legislation should impose adequate data security obligations on the data controller for the duration of such storage. Most data protection legislations have provisions such as:

The data controller must ensure that the data is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse.
The integrity of personal information to be secured by taking appropriate technical and organisational measures.
Steps should be taken to prevent unauthorised access to personal data, including the right of physical access to the premises, data, and programs and to operate equipment of the data controller or processor.
The identity of persons who have access to information network should be logged.
The organisation must appoint specific staff (such as a security officer) to maintain security of data and prevent the data from burglary, alteration, destruction, extinction, or disclosure.

Some laws also mandate technical procedures and measures to protect data while in transmission. This includes an obligation to transfer data only in cryptographic form with a digital signature.
In some countries, the data regulator is responsible for ensuring credibility and integrity of the data controllers handling the information and for ensuring that equipment used is of a high standard.
Some countries also vest an obligation on organisations to inform data subjects of security incidents that may lead to a threat of unauthorised disclosure of personal data.
Privacy impact assessments to be conducted by independent authorities in the form of transparent audits, for the protection of personal data.
Adoption of a code of practice to measure the efficiency and level of protection of personal data.
A response plan to be formulated by organisations which will set out the appropriate action to be taken for breach of data protection laws.
The technical and organisational measures to be undertaken by data controllers must be proportionate to the existing risk, sensitive nature of information and its consequence for the data subject.
When processing is carried out by service providers, the controlling authority must enter into a contract that provides the scope, content, obligations and guarantee of compliance of data protection principles by these service providers.
At the time of encountering a security breach during processing, the data subjects must be informed about the potential pecuniary and non pecuniary effects of such a breach. This information must be provided well in advance.
Mechanisms that prevent and detect breaches depending upon the standardised model of information security governance/management must be implemented.
Periodic internal training, education and awareness programmes aimed at better understanding of data protection principles and security issues must be implemented.
Data privacy officers with adequate qualification, resources and power for supervisory functions must be appointed to overlook functioning of data controllers.
Response plan that establishes guidelines for verifying a breach of applicable law, cause and extent of breach, harmful effects and appropriate measures to avoid future breaches must be implemented.
Data supervising authorities must ensure the following security standards are maintained:
(a) Supervisors must be impartial, independent and have technical competence and adequate resources to carry out their functions;
(b) Supervisors must ensure coordination to achieve uniform standards of data protection is maintained at national level, by sharing reports, investigative techniques and other necessary information; and
(c) Supervisors must maintain high level of confidentiality of information exchanged during course of co-ordination.

Recommendations

To the extent possible **the legislation must prescribe the measures to be taken by the data controllers to ensure the security of data under its control**. Care should be taken to ensure that the measures prescribed should be technology neutral as it is likely that data security measures will only improve in the future. The emphasis should be on ensuring that appropriate measures are taken with a view to achieving a prescribed and stated result. There should be no attempt at prescribing the means to achieving that end.

It is recommended that the data must be protected again unauthorised access, deletion, disclosure and alteration. The onus to protect the data must be on the data controller. It may also be worth considering circumstances under which the data regulator could supervise the implementation of these measures.

9.9**Data Access**

Once data has been collected it remains under the control of the data controller. If the data changes (such as in the event the data subject moves to a different address) it is important that this data be rectified and made current. Similarly, if the data subject finds, after his data has been collected, that the database entries are incorrect, it should be open to the data subject to rectify the database in order to rectify his own data. Many data protection legislations include provisions such as:

Data subject must have access to the data, subject to applicable laws. The subjects are also granted the right to rectify.
In some countries, the correction of personal information can be made following an investigation.
Some countries have an exception that records maintained in anticipation of a civil action or proceeding cannot be accessed.
Some countries require that the data holder must produce relevant identity proof while requesting access to personal data.
It is mandatory for the data controller to provide an individual with information with respect to data controller, the purpose of data collected and who are the recipients of the data, information on processing of the data etc.
Information must be provided to the data subject in an intelligent form using clear and plain language. Special care must be taken with respect to information of minors.
National law may restrict the repetitive exercise of access of information within a short period of time, unless data subject provides sufficient reasons.

Recommendations

In order to ensure that the database is accurate and up to date, specific provisions should be included to allow data subjects to rectify their own personal information. In fact, data subjects should always be allowed to review their personal information collected and stored in the database.

It is important to consider whether legal heirs, guardians and authorised representatives of the data subject should be granted access to personal information of their guardians or wards. This would also be relevant to consider in the context of deceased data subjects – for instance, would it be possible to conclude, after the death of a person, that he ceases to be a natural person and therefore is no longer protected under the statute? In all these circumstances adequate verification procedures must be implemented to ensure that personal information does not fall into the hands of persons not authorised to collect it.

9.10**Cross Border Applicability And Transfer**

European countries extend the applicability of their data protection legislations to persons who may not be located within the country but may be using equipment located in the country, to process information. Most European legislations also prohibit the transfer of data to countries with less rigorous data protection laws. Our review indicates that 66% of countries analyzed, have provisions that permit the regulator to prosecute non-residents in respect to data offences as long as the data in question is stored within the country and the storage was not merely for the purpose of transit.

Recommendation

A strong data protection law will afford the opportunity for free flow of personal data from the European Economic Area to India. This would particularly benefit providers of outsourcing services located in India. However, there may not be a pressing need to enact data protection legislation as stringent as the European legislation in the Indian context. While there are many benefits in having a strong regime, the practical difficulties in implementing such provisions in a country of over a billion people with not prior experience in data protection would be challenging in the extreme.

However, it may be advisable to ensure appropriate measures to protect the data of Indian citizens that are processed outside the country. The legislation could include provisions that allow the regulator to proceed against data controllers not just for data protection violations committed within the country but also outside the country if the data concerned relates to an Indian citizen, or was collected by the data controller in India.

9.11**Exemptions**

All data protection legislations have in-built exceptions that limit the applicability of the legislation in the context of certain statutorily established circumstances. These could include national security interests, statutory functions, disclosures required by law or as part of legal proceedings, etc. There could be several specific exemptions that are particular to the Indian social and economic environment.

On an examination of the data protection enactments around the world, the most common exemptions are on grounds of national security, adopted by 65% of nations examined, followed by prevention and detection of crime at 58%. Most countries also provide exemptions for the purpose of apprehension and prevention of offenders, protecting the public from financial loss, protecting charities against mismanagement, disclosures required by law or under legal proceedings, securing the health, safety and welfare of people at work, statistical or historical research purposes, assessment of collection of tax, processing for the publication of journalistic, literary or artistic material and discharge of a statutory function from the principles of data protection.

Recommendation

In the Indian context, it will be important to include exemptions on grounds of national security, discharge of statutory functions, protection of health and safety of citizens and such other circumstances as appropriate. However, in articulating exceptions care must be taken to ensure that the purpose for framing of the legislation is not diluted so much as to make it meaningless. Thus, while national security exemptions are necessary and recommended, they should be framed carefully to ensure that it is not possible for just anyone to claim that the provisions of the law are not applicable by citing some national security interest without substantiation. The persons who can claim the exemption and the circumstances should be carefully limited.

9.12 **Automated Decision Making**

As discussed earlier in this document, given that personal data is collected and stored digitally, it is possible to process this information automatically using computer algorithms designed for that purpose. This form of processing is completely objective and based solely on the information provided. As a result, the decisions taken could lead to unfair results in circumstances where all the information is not provided or where additional relevant information does not form part of the evaluation algorithm. All European data protection legislations have provisions that deal with this addressing the concern in a variety of different ways. Some examples of how international statutes deal with automated decision making are listed below:

A request to stop the processing can be made with proof that the result would be against the vital interest of the individual.
Processing which reflects aspects such as credit worthiness, conduct, performance etc. cannot be logically processed in an automated manner.
The data subject has the right to understand the logic of the automated decision making algorithm.
The data subject has the right to request the physical supervision over processing through automated means.

Recommendation

While there may not be an immediate need to include provisions relating to automated decisions into the data protection legislation (given the relatively few instances – if any – where data subjects have objected to such decisions having been taken against them), it is likely that as we grow more and more reliant on electronic databases this will become more of a problem. With that in mind it will probably be useful to include these provisions into the legislation.

9.13**Regulatory set up**

Most countries that have adopted data protection legislations have established a special regulator to deal with contraventions of the legislation as well as to more proactively supervise compliance with the statute. The regulator also prescribes the standards against which compliance is measured and is called upon to adjudicate disputes in relation to the provisions of the law.

The extent to which a data regulator is required in the context of an Indian data protection legislation will depend to a large extent on the shape of the legislation. In the event it is intended that the law should operate as an umbrella legislation under the terms of which various sector specific legislations would spell out the more detailed sector oriented issues, then a regulator would be required to harmonise the provisions of the data protection law with the sector specific legislations. Where the legislation spells out the broad principles for data protection, it will be left to the data regulator to articulate the specific regulations that apply

There are 3 options regarding setting up a regulatory mechanism to enforce the law:
Heavy handed Regulation through a separate regulator
Light handed regulation through office of Ombudsman and reliance on self regulation by government and industry bodies.
Converting existing Information Commissions into privacy and information commissions who will enforce the legislative provisions.

Data Security Council of India (DSCI) has recommended that the proposed privacy Act should incorporate the privacy principles that should form the basis of privacy protection of individuals both by the public authorities and private corporate, NGOs and other entities that collect personal data. It should establish the office of a Privacy Ombudsman (PO) and recognize the role of industry associations as Self Regulatory Organizations (SROs). The privacy codes established by the SROs will be vetted by the Ombudsman. He will also validate the Alternative Dispute Resolution (ADR). However, neither the Ombudsman, nor the SROs investigation reports on disputes will be binding on the disputing parties. In the event of non-acceptance by either party to the dispute, they are free to go to a court of law. The PO will oversee the implementation of privacy regulation across the country. The PO will be responsible for issuing guidelines on privacy principles, in consultation with the industry.

Recommendation

In the Indian context it is advisable to establish a regulator under the proposed data protection legislation. The role of the regulator would be to ensure that the legislation responds dynamically to the changing digital environment and fulfills the principles upon which the legislation was based. To this end the regulator should have the power to prescribe standards both technological and operational that could mould the manner in which the legislation is implemented. It is particularly important to develop the concept of accountability so that it should no longer be sufficient for organisations to meet applicable data protection requirements – they should demonstrate their willingness and ability to take on data responsibility and ensure compliance on an ongoing basis. The regulator should also have the power to require subsidiary regulators who operate under the provisions of legislations that include reference to data protection principles, to

conform to the broad principles of the data protection legislation.

Since data protection and personal privacy are the other end of the spectrum from the right of citizens to access public information (as enshrined in the Right to Information Act), it may be appropriate to house the office of the Data Regulator within the same executive framework as the chief information officers under the Right to Information Act.