

2013

Protecting The Unprotectable



DISCLAIMER

This Article is a Copyright of Kaushal Shah & Associates. No reader should act on the basis of any statement contained herein without seeking professional advice. The author and the firm expressly disclaim all and any liability to any person who has read this article, or otherwise in respect of anything, and of consequences of anything done,

Kaushal Shah & Associates is a boutique law firm located in Mumbai the commercial capital of India, which provides a unique service by focusing on effective discussion, careful listening, skilled and systematic planning process to approach our work. Based on our knowledge of key industry sectors and legal practice, the Law Firm provides holistic, innovative flexible commercial solutions to result in good transaction management.

The Law Firm is distinguished by its unsurpassed expertise in Corporate, Media Entertainment and Sport, Private Equity and Venture Capital Investment Funds, Intellectual Property, Human Resource, Life sciences, Technology and Real Estate. Each of our associates has expertise in specific area of law and is a leader in one's own field. Each of our specialist teams has a wealth of knowledge and practical experience.

At Kaushal Shah & Associates, we offer more than just law. We make it our business to understand your business and complex legal problems. We aim to be an integral part of your organization and place our emphasis on working closely with you to achieve your business goals through our sound, distinctive culture that puts people first. We believe that cultivating relationships is the key to our success.

406, Peninsula Plaza, Funrepublic Lane, Off Andheri Link Road Andheri (W)
Mumbai 400 053. Tel: +91 22 267 333 94 Telefax: +91 22 401 098 21
E-mail: Kaushal@ksaattorneys.com
Url: <http://www.ksaattorneys.com>

Introduction

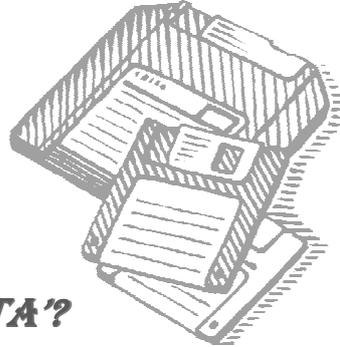


In the new era of globalization, growth of industries has advanced the technological development with knowledge process outsourcing and has surfaced a new threat of illegal activity than letting the masses experience its benefaction. Seeing the growing trend, the majority of essential information e.g. such as the trade secrets of a firm, are kept in electronic form. Data transfer between countries has been a burning topic all over; however, various incidents of data theft and misuse of private and personal information have raised concerns about outsourcing to India. In the present phase where technology drives human lives, most of the crimes

are being committed through the easiest medium i.e. Computer and Electronic gadgets and which are famously known as **Cyber Crimes**.

Thus in India, the absence of any particular stringent laws on the Data Protection has invited a very big trouble for every entity, be it a governmental body, financial institution, business houses or even a lay man, to give adequate protection to their huge data bases as maintaining it is not as much a difficult task as maintaining its integrity. Through this article we would like throw light on the efforts in **Protecting The Unprotectable**, which is the subject matter for today's era.

Therefore, to make you all aware of the bone of contention in privacy infringement let us begin by explaining the concept of what data is and its essentiality.



Meaning:

WHAT IS 'DATA'?

To be precise, Data is a piece of knowledge or information stored in any form, its “a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed,

is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer”.

Now the forthcoming predicament is its

Emerging need:

The increasing popularity of Internet brings us to a world of dilemmas. Pros of using it are well known, but there are many cons that diminish them. Some problems appeared in the last few decades and there is



an urgent need to introduce legislation devoted to law and social issues taking into consideration this powerful medium.

The purpose of data protection legislation is to ensure that personal data is not processed without the

knowledge and, except in certain cases, without the consent of the data subject, to ensure that personal data which is processed is accurate, and to enforce a set of standards for the processing of such information.

It is to protect living individuals against the misuse of their personal data. Examples of such misuse could include exposing of personal data without obtaining prior permission from the data subject, holding incorrect and

Current scenario:

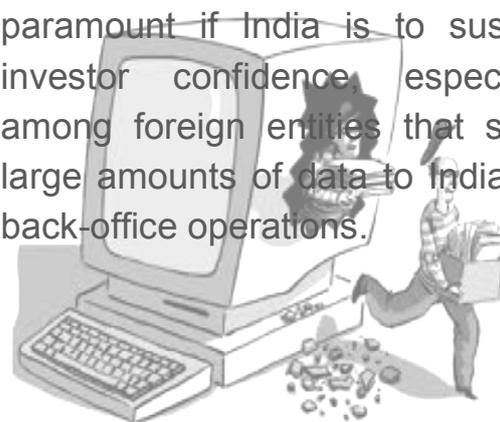
It is noticeable that information system can not only improve company's operating, but it may also become a serious threat. We can safely estimate that nowadays every company, no matter how big it is, uses internet for marketing or communication purposes.



Transparency, accountability and data protection are all

possibly damaging personal information and unauthorized alteration of personal data and also to decrease public concerns over the level of confidentiality of their data held at various organizations.

The need for data protection is paramount if India is to sustain investor confidence, especially among foreign entities that send large amounts of data to India for back-office operations.



essential elements for awesome governance.

To achieve this objective, the Government felt the need to enact the Data Protection Act and so has proposed the Personal Data Protection Bill, 2006 which has been introduced in the Parliament to codify the laws on Data Protection which presumably will be passed in the upcoming time intending to strengthen the fundamental rights of every individual and also to tackle issues that previously were unregulated

The personal data protection bill 2006:

The purpose of the bill is to provide for the protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to

disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Data controllers have been proposed to be appointed to look upon the matters relating to violation of the Bill.

Therefore, it can be said that the proposed Legislation for Data Protection will ensure adequate safeguards.

DATA PROTECTION AND PRIVACY RIGHTS:

We would like to mention that in the absence of specific legislation, data protection in India is achieved through the enforcement of privacy and property rights. Privacy rights are enforced under the Indian Constitution ("Constitution") and the Information Technology Act 2000, whereas the Indian Contract Act, 1872, the Copyright Act, 1957, and the Indian Penal Code, 1860, protects property rights.

THE INDIAN PENAL CODE, 1860 (IPC)

Can be used as an effective means to prevent Data theft. Offences such as misappropriation of property,

theft, or criminal breach of trust attract imprisonment and fine under the IPC. Although the offences of theft and



misappropriation under the IPC only apply to movable property, it has been defined to include corporeal (TANGIBLE) property of “every description,” except land and things

permanently attached to the earth. Therefore, computer databases can be protected under the IPC, as they are movable by their very nature and under the Copyright Act because they are a form of IP.

THE LAW OF CONTRACTS:

These days’ companies are relying on the law of contracts as an essential means to protect their information or personal data. The corporate houses in India enter into the several agreements with other companies, clients, agencies etc to keep their information secured. The most common prevalent practice amongst Companies in India is entering into lawful binding Contracts. Contractual obligations are widely practiced alternative followed in India to ensure Data Protection.

Agreements such as non-disclosures, non circumvention, User-license, User Source Code Agreements, Referral Partner agreement etc. are entered into by them to ensure confidentiality and privacy clauses there by putting up an effort to secure data. In addition to the Contractual protection, The Specific Relief Act, 1963 provides for preventive relief in the form of temporary or permanent injunction for breach of obligations and also damages are awarded under the same act.

INDIAN CONSTITUTION:

Our constitution has provided the law relating to privacy under the scope of Article 21 which provides for a fundamental right to life and personal liberty. This Article is capable of a wider and multiple

scope of interpretation. Judicial activism and the Supreme Court of India has from time to time interpreted that the right to life and personal liberty means to include inter alia right to privacy. Thus,

interpretations of this Article will extend to the right to protect Personal Data. However, this Article is not absolute and can be curtailed in accordance to procedure established by law but it acts as a supportive constitutional provision forming base for the other relating laws apparently

filling the wide lacuna of Data Protection Laws. This Article can only be invoked against the State Government or Central Government. Both the Supreme Court and High Courts of India have power to decide any matter under Article 21

THE INFORMATION TECHNOLOGY ACT, 2000 (“IT ACT”):

In the year 2000 effort has been made by our legislature to embrace privacy issues relating to computer system under the purview of IT act, 2000. This act contains certain provisions which provide protection of stored data. The Preamble to the IT Act states that the act is enacted to provide legal recognition to electronic transactions and transactions which are an alternative to the paper based methods of communication and storage of information. The Preamble of the act has wide scope of interpretation creating room for ambiguity and multiple interpretations. The IT Act although doesn't have any specific

provisions in respect of Data Protection but there are certain provisions provided in the IT Act which can ensure minimum though not specific protection to Personal Data.

Here, we have made an effort to enlighten you on these provisions by discussing them in detail.

Section 43: this section provides for the protection against unauthorized access against the computer system by imposing heavy penalty up to Rupees One Core (Rupees 10 million), The section also covers the unauthorized downloading, extraction and copying of data, with the amendment of this section

further a pecuniary penalty has been awarded in event of failure to protect data inter alia inclusive of sensitive personal data.

Further, Section 65: discusses for the computer source code. Who so ever knowingly or intentionally conceals, destroys, alters or abets another to do as such, shall have to suffer a penalty of imprisonment or fine up to Rupees 2 Lakh (Rupees 200 thousand). Thus protection has been provided against tampering of computer source documents.

Section 66: talks about HACKING and Protection against hacking.

hacking may be defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss of damage will be caused to any person and the information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished.

This section imposes the penalty of imprisonment of three years or fine up to Rupees Two Lakh (Rupees 200 thousand) or both, on the hacker. The amendments to Information Technology Act,

2008 have inserted Section 66 B for punishing the dishonest receiving of stolen computer resource or communication device.

Section 70: provides protection to the data stored in the protected system (computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system.) Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

and lastly with Section 72: which deals with the protection against breach of confidentiality and privacy of the data, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material, discloses it to any other person, shall be punished with imprisonment which may extend to

two years or with fine which may extend to One Lakh rupees (Rupees 100 Thousand) or both. In accordance to Amendment to the Information Technology Act 2008, section 72 (A) has been

inserted which imposes punishment and penalty for disclosure of information in a breach of lawful contract.

Therefore seeing all the above sections we can clearly say that though the act is enacted to provide legal recognition to electronic transactions, it still fails to provide for a comprehensive protection to Personal Data.

A FRIEND CUM ADVISOR, THE NATIONAL ASSOCIATION OF SOFTWARE AND SERVICE PROVIDER COMPANIES (NASSCOM):

NASSCOM acts as an advisor, consultant and coordinating body for the software and services industry in India. NASSCOM aims at enabling Indian Information Technology/ Information Technology Enabled Services (IT/ITES) organizations to provide high standard of security and data protection, build capacity to provide security certification to organizations, to provide common platform for promoting knowledge

about information security and foster a community of security professionals/firms and create awareness among industry professionals and other stakeholders. NASSCOM has acted in an advisory capacity to the Government of India in the drafting of the Information Technology Act, 2000 and currently is an active advisory to the Ministry of Information Technology, India advising on the current need of Data Protection Laws.

A COMPARATIVE ANALYSIS OF THE PERSONAL DATA PROTECTION LAWS WITH EU, US AND U.K

There are three basic principles on Data Protection to be common and extremely important viz.

that the data should be collected with the express consent of data subject;

the data should be collected for specific purpose and it is to be processed only for that purpose;

The data subject should have access to his data for making factual amendments to it.

Transborder flow of information is extremely important as countries will not have the option to avoid data protection. To allow such trade to continue, countries around the globe, it must implement privacy policies of their own and consider how they will protect the information of their citizens as well as the personal information they receive through onward transfer. In wake of commercial globalization and trade, the EU directives have created a primary base for Data Protection and more countries are enacting Data Protection Legislatures/Statutes/Acts to be in terms with EU union Data Protection laws. The U.K laws on

data protection are in tune with the EU directives. Both the U.K laws and EU directives have created certain platform for other global economies to follow suit in enacting the data protection laws. Most of the European Union member states have Data Protection

Legislatures/Statutes/Acts in lines of the EU directives.

Owing to the advent of cloud computing, online social networking, internet surfing etc. the existing data protection laws do not provide protection for the complexities that arise of it. The European Commission realizing this complexities are in a process of reviewing the EU directives to suit the need of the hour and strengthen individual privacy rights as well as to ensure protective usage of data. The United Kingdom laws on data protection being of complex nature also need reformation

In order to be in tune with the EU directives, U.S Department of Commerce created Safe Harbor Program and the Privacy Act, 1974. The states like California

have enacted Data Protection Laws. However, there are certain federal Bills like 'The Commercial Privacy Bill of Rights Act, 2011', 'Do-Not-Track Online Act of 2011', 'Data Security and Breach Notification Act of 2011', etc. that are pending and being considered by the U.S senate. The passing of these Bills will try to encompass the laws of data protection in consonance with the other major economies of the world. Despite the above mentioned legislations, U.S still needs to have a basic federal legislation on data protection, strengthening individual's right to privacy, which will act as supreme to all the other 'sectoral' legislations.

As far as India is concerned, Contractual obligations on confidentiality and data protection and the IT Act (to a limited extent) embodies though not stringently the concept of Data Protection. The Personal Data Protection Bill,

2006 envisages the concept of Data Protection in lines of EU directives. The Bill when passed will be India's commendable step towards commercial globalization and will surely ensure stringent laws on onward transfer, collection, exchange, processing etc. of personal data and other information, thereby, ensuring Data Protection of international standards. The Bill, though being the first ever codified legislation on data protection in India, has been so drafted so as to adhere to the EU directives and hence it is quite similar to the U.K. law on Data Protection. However, it fails to cover future hurdles in the flow of data due to globalization. India's growing economy today, in our opinion, needs a comprehensive data protection law which is a compilation of both the EU directives and the U.S. laws.

CONCLUSION

In the coming years it will be increasingly necessary to consider the implications of the Data Protection Laws in India. Data

differs from one another on the basis of its utility. It is not of same importance to everyone. On comparing the Indian law with the

law of developed countries the proper requirement for the Indian law can be analyzed. The companies cannot get full protection of data in the absence of data protection laws which ultimately forced them to enter into separate private contracts, to keep them secured and to ensure the safety of their clients. These contractual and confidential agreements have the same enforceability as the general contracts have. The Data Protection Legislation/Act/Statute is in place for a smooth functioning of the International trade and economy. The Personal Data Protection Bill, 2006 when effective will serve the purpose of protecting the data from its misuse

which might cause heavy losses to any entity who is the data subject. Despite of all these efforts made by our legislature, for having the data protection law as a separate discipline, our legislature has still left some lacuna in framing this bill therefore, being the most concerned topic of discussion in the modern era, legislature are required to frame more stringent and comprehensive law for the protection of data which requires a qualitative effort rather than quantitative

Thus we can conclude that a complied law on the basis of US and UK would be more favorable for today's requirement.

wikipedia.org/wiki/Data_Protection_Act

Asian School of Cyber Laws, study material on Diploma course of Cyber Laws.

legalserviceindia.com/article/I37-Data-Protection-Law-in-India.html