Is Your Data Safe?

Vanishing of virtual boundaries led to open availability of personal and private information. The new IT Rules 2011 have been notified after the 2008 amendment of IT Act 2000 to address the issue of protection of data collected besides many other important issues. Find out whether the rules are good enough to usher in a new data protection regime in India

Stuti Bansal

India, of all the countries, has more than one requirement to be tied down by stringent and well defined data privacy laws. By offering cheaper and smarter workforce to suit the requirements of business outsourcing, India has become one of the most preferred destinations for offshore business outsourcing. The privacy and protection of this data is becoming a concern for the advocates of privacy. Moreover, with the advent of cloud computing and all the preparations to use it to the most, the need to ensure data privacy just keeps increasing and will gain more prominence with the passage of time.

CONCEPT OF PRIVACY

Privacy is said to be the "Right to be let alone". The Constitution of India does not explicitly grant or guarantee the fundamental right to privacy. However, the Supreme Court and the other courts in India have read and related the Right to privacy with the other existing fundamental rights, i.e., Freedom of Speech and Expression under Article 19(1) (a) and Right to Life and Personal liberty under Article 21 of the Constitution of India. The Supreme Court has, in the cases of Kharak Singh vs State of Uttar Pradesh and Gobind v State of Madhya Pradesh, recognized a right to privacy derived from constitutional rights to speech, to personal liberty, and to move freely within the country. However, these Fundamental Rights under the Constitution of India are subject to reasonable restrictions given under Article

19(2) of the Constitution that may be imposed by the State. Privacy forms a very important part of the laws of most jurisdictions, treaties and agreements. The right to privacy in India has derived itself from essentially two sources: the common law of torts and the constitutional law.

It has been said that privacy is important because it is:

a. A way of controlling the power which people or organizations gain through collecting and storing information about others,

b. A means of securing the trust which people expect in return for providing accurate information about themselves,

c. A necessary condition for living in a society which values freedom and diversity,

d. The basis on which we form meaningful relations with other people by deciding how much of ourselves to reveal or conceal to any given person.

Besides these, privacy is internationally recognized as a basic human right, for example, in the Article 12 of the United Nations Universal Declaration of Human Rights. Furthermore, Article 17 of the International Covenant on the Civil and Political Rights 1966 is almost identical to Article 12 of the UNDHR.

DATA PROTECTION

The Information Technology Act, 2000, giving recognition to electronic records and data, provides a typical yet not specific framework of laws relating to data protection. Section 43 of this Act imposes a penalty of one crore rupees on any person copying or extracting any data or computer data base information from a computer, computer system or computer network, including information or data held or stored in any removable storage medium. Further, Sections 65 and 66 also provide for penalties in cases of damage or tampering of data stored in computer systems. However under Section 69 of the Information Technology Act, 2000, an exception to the general rule of maintenance of privacy and secrecy of the information has been provided wherein if the Controller appointed under the Act by the Central government, is satisfied that it is necessary in the interest of the sovereignty or integrity of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may by order, direct any agency of the appropriate government to intercept and monitor any information transmitted through any computer resource.

VOICE

VINEET VIJ
Head Legal , HCL Technologies Ltd.

A strong regime of data protection in India!

Subsequent to the enactment of Information Technology Amendment Act, 2008, No. 10 of 2009 ("ITAA 2008") which set the ball rolling for addressing the lacuna of data protection laws in India through sections 43A and 72A, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Privacy Rules/Rules") issued in April last year to implement the ITAA 2008 impose significant limitations on how body corporates can handle personal information of individual customers. These Privacy Rules align India with other countries having various data protection laws/regimes viz. Data Protection Act (UK), Directive 95/46/EC (Europe), GLBA and HIPPAA (USA) etc, all of which deal with personal identifiable information. Indian Privacy Rules bear strong resemblance to EU Rules in terms of data access, data retention, purpose limitation and imposition of mandatory data privacy standards for adequate protection of personal data.

Undoubtedly, these new Rules are a step forward, helping to bring India in line with EU practices which will give further comfort to individual customers of Indian service providers that their personal data is secure. In practice, overseas outsourcers are unlikely to see a step-change with these Rules not being applicable to them, as also their Indian service providers already comply with best practices to meet their customer's requirements, though such overseas outsourcers would be reassured by recent developments which bolster the additional protections Indian companies must put in place in order to provide services to Indian individual customers. Despite ambiguities around implementation of these Rules and non-existence of a national regulatory body to specifically oversee the enforcement of privacy protections, stage has been set for a strong data protection regime in India. I am also optimistic that lacunas would be appropriately addressed through legislative enactments and judicial pronouncements.

... as told to Khalid Perwez of Lex Witness

However, these provisions of the Act were not stringent enough and provided a weak system of security to protect data. Remedying this, the Information Technology (Amendment) Act, 2008, enacted on 27.10.2009, made many insertions and substitutions in the existing legislation. Some noteworthy amendments include the introduction of the term cyber security, provision for compensation in case of failure to protect data (Section 43A), punishment for violation of privacy (Section 66E), punishment for cyber terrorism (Section 66F), and many more. These amendments made the law stronger and gave it more weight. Where until April 2011, no data privacy protection laws, whether comprehensive or sectoral, existed in India, and no regulator had been established to issue, administer, and enforce data privacy rules, the Ministry of Communications and Information Technology vide notification No GSR 313 (E) dated 11th April 2011 made the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("The Rules").

INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES 2011

These Rules have been framed in furtherance of Section 43A of the Information Technology Act, 2000 which relates to the protection of individual data. For the first time, the Rules in order to protect data in India, mandate a Body corporate or individual collecting, receiving, processing, storing, dealing or handling information to provide a policy for privacy and disclosure of information.

A clarification regarding these Rules was also issued by the Ministry of Communication and Information Technology saying that the newly- enacted Rules apply only to companies and persons located in India and companies that collect data directly from customer. Further, it clarifies that any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India, except those providing services to the provider of information under a contractual obligation directly with them, shall not be subject to the requirements of Rule 5 (Collection of Information) and Rule 6 (Disclosure of Information). The Press Note clarifies that privacy policy, as prescribed in Rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract.

Interestingly, and for the first time, the Rules provide for the definition of "Sensitive Personal Data or Information" as including information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of password, user details as provided at the time of registration or thereafter, information related to financial

Q&A

STEPHEN MATHIAS
Partner, Kochhar & Co, Bangalore

Could you throw some light on the IT Rules 2011 that propose to bring about a strong system of data protection?

These rules come out of section 43A of the IT Act which permits the government to notify "reasonable security practices and procedure" that one might follow in order to avoid liability in a situation of wrongful loss or gain arising due to failure to protect data. The rules are much wider in scope that what appears to be contemplated by the statutory provision, are badly written and are clarified by a clarification from the Government which is also badly worded. It is unclear to what extent these rules need to be followed and even how aspects of the rules would be followed in specific situations. Overall, it is recommended that parties who are concerned about these rules understand first the background to section 43A, the risks involved in not complying entirely with the rules and then take a decision on the extent to which they wish to comply. We advise companies to ensure they have robust systems in place to protect data and to meet basic global standards on privacy – agreeing with the party providing the data as to who will access the data, what it would be used for, etc.

Do you think these rules will bring about any significant change?

The notification of these rules has heightened awareness among businesses about the need to protect personal information of others available with them and to have a privacy policy/agreement in place with such persons. This is the overall beneficial effect of the rules. Because the very basis for the rules is questionable and they are so badly written, there is a huge negative effect – confusion about whether to and how to comply with the rules.

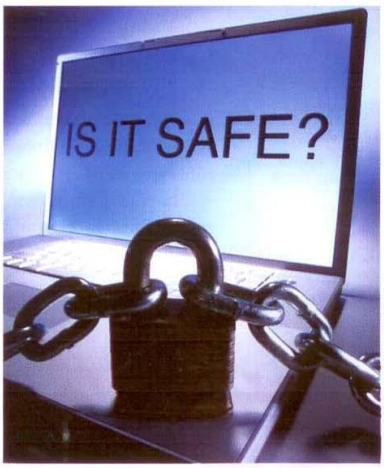
...as told to Khalid Perwez of Lex Witness

information such as Bank account / credit card / debit card / other payment instrument details of the users, physiological and mental health condition, medical records and history, biometric information, information received by body corporate for processing, stored or processed under lawful contract or otherwise and call data records.

With respect to the security and handling of this Sensitive Personal Data or information, the Rules provide many instructions, mandates and obligations. Apart from mandating the provision of a Privacy Policy for the use of information by the body corporate or person collecting information, the Rules also make provisions regarding collection of data. Detailing this provision to ensure public knowledge, Rule 4 of the Rules such Policy must be published on the website of the body corporate or any person on its behalf and should provide 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 including sensitive personal data or information and reasonable security practices and procedures. The Rules thus make every attempt to instruct every body corporate or individual collecting information to follow a route of action and provide every detail about the way it envisages to use the information provided.

It is provided that the collector of information, whether body corporate or individual, must ensure that the information is collected for a lawful purpose and the provider of the sensitive data or information be informed that data is being collected from him and the purpose of the collection of such data, as also the intended recipients of the information.

Regarding disclosure of information, the Rules provide that disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such



Sensitive personal data or information may be transferred to another body corporate or individual in India or located in any other country, only where such entity maintains the same level of data protection as is prescribed in the Rules.

information, who has provided such information under lawful contract or otherwise. The only exceptions to this are where such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

Sensitive personal data or information may be transferred to another body corporate or individual in India or located in any other country, only where such entity maintains the same level of data protection as is prescribed in the Rules.

Further, a company shall be considered to be in compliance of the Rules where they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

IMPACT AND CONCLUSION

In an attempt to meet the global standards relating to data protection and privacy, the Rules 2011 provide a fairly concrete and much awaited and required framework of laws. One of the concerns that may however arise is relating to the use of the words "provider" of Information. The Rules use the term Provider which does not always give enough protection to the person whose information it is or to the person to whom the information relates. Where the provider of information is different from the person to whom the information relates, there may arise misunderstanding and again, misuse of data.

However, with no particular and specialized statute dealing in handling of personal data, the notification of the IT Rules 2011 come as a welcome move in the wake of the increase in activities and transactions relating to data collection and also highlights the growing importance of data security. With each industry cashing in on reaching out to people through their relevant personal information, the Rules are a ray of hope to the information provider and owner of information.

ABOUT AUTHOR

The author is an allumunus of Symbiosis Law School, Pune, and working as Associate Advocate at Corporate Professionals, Advocates & Solicitors, a corporate law firm in Delhi and also pursuing the course of Company Secretary.