DataGuidance
GLOBAL GUIDANCE IN ONE

GUIDANCE NOTES

India - Data Protection in the Financial Sector

Huzefa Tavawalla and Kartik Maheshwari
8 July 2014

1. Introduction

An increasing number of Indians are now using digital payment solutions to transact over the internet. According to a recent research report published by the Internet and Mobile Association of India (IAMAI) in association with the Payments Council Of India (PCI) and IMRB , the digital payments industry is expected to grow over INR 1.2 trillion (approximately $20 billion) by December 2014.

Financial services, including banks, credit card companies, insurance, micro finance institutions and securities trading, are all increasingly moving business online and the common feature of all such services is that they require critical information to allow the user to transact. Thus, the kind of information required by this sector coupled with the large Indian population taking to the internet to manage their finances puts a lot of personal data in the hands of the service provider.

With the rise in digital payments, financial institutions and especially Indian banks have also increased their efforts to ensure that the entire process is more robust and error free. In this context, banks alone are expected to spend nearly INR 447 billion (approximately $7.4 billion) on IT in 2014 . However, the risks associated with the increasing adoption of technology in the banking and financial services sectors have also increased manifold. According to the Trend Micro Q3 Security Round-up Report 2013, online banking malware volume surged this quarter, with a huge 253% increase in online banking malware Infections in India in Q3 as compared to Q2.

2. Broad Legislative Framework

While there have been news reports about the Indian Government contemplating the introduction of a comprehensive legislation on privacy since 2010, this has not yet been formally introduced as law. News reports as recent as April 2014 have once again suggested that the government is considering the introduction of the much delayed privacy bill and it is hoped that such law will be formalised shortly.

Fundamentally, the Supreme Court of India has, in various decisions, recognized the right to privacy implicit in the right to life granted under the Constitution of India and therefore privacy is accorded the highest protection under law. Such constitutional remedy, however, is only available in response to an action taken by the state.

Specifically, there are other independent laws and industry guidelines which accord protection, however, the access, collection and usage of sensitive personal information in e-form is governed by the Information Technology Act, 2000 ('**the IT Act**').

A mandatory data protection regime dealing with sensitive and personal data in India was brought into force with the introduction of Section 43a as part of the Information Technology (Amendment) Act, 2008. This 2008 amendment was introduced to allay fears concerning the safety of sensitive data or personal information being transferred, collected or handled by Indian companies. Such a data protection regime was also considered essential to support the growth of the burgeoning Indian IT sector and business process outsourcing as well as to bring the Indian regulatory framework in line with various global legislations on this topic. Consequently, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ('**the Rules**') were also enacted to build a more robust and comprehensive regime regarding the protection of sensitive and personal data.

The Rules accord protection to Sensitive Personal Data or Information (**SPDI**) which essentially consists of personal information relating to:

1. passwords;
2. financial information such as bank account or credit card or debit card or other payment instrument details;
3. physical, physiological and mental health condition;
4. sexual orientation;
5. medical records and history;
6. biometric information.

The Rules lay down various procedures and obligations which need to be observed at the time of collection, transfer or disclosure of SPDI along with certain required reasonable security practices and procedures. It is important to note that any liability arising hereunder is uncapped, subject to the discretion of the courts. The courts would usually determine the liability depending upon the severity of the loss caused to the aggrieved person.

Also, Section 72a of the IT Act introduced in 2008 covers personal information *(information*

About The Authors

Kartik Maheshwari is an Associate at the international law firm Nishith Desai Associates. Nishith Desai Associates have been recognised by Legal 500 and Chambers and Partners and have also received the award for Most Innovative Indian Law Firm by Financial Times in its 2014 study of Innovative Lawyers across Asia-Pacific including Australia (APAC).

Mr. Maheshwari is a member of the Corporate and TMT teams. Mr. Maheshwari assists clients on complex cross border mergers and acquisitions, fund investments and joint ventures. He also frequently advises clients on general commercial laws and has assisted global software vendors with their negotiations and drafting of their agreements with Indian companies along with regularly advising clients on the Indian data protection regime. Mr. Maheshwari was seconded to the offices of a large US based technology company helping them structure and setup their operations in India.

Mr. Maheshwari graduated from Symbiosis Law School, Pune and is a member of the Bar Council of Maharashtra & Goa.

Email:
Kartik.Maheshwari@nishithdesai.com

Huzefa Tavawalla is a Principal Associate at the international law firm Nishith Desai Associates. Nishith Desai Associates have been recognised by Legal 500 and Chambers and Partners and have also received the award for Most Innovative Indian Law Firm by Financial Times in its 2014 study of Innovative Lawyers across Asia-Pacific including Australia (APAC).

Mr. Tavawalla is a senior member of the TMT & Corporate Practice Groups and focuses on matters pertaining to Intellectual Property, Information Technology, Media & Entertainment, Telecommunication, Mergers & Acquisitions and International Tax.

Mr. Tavawalla has been at the forefront of outbound and global M&A in particular project management for large cross border acquisitions. Further, he has advised on several cutting edge, complex and cross-border telecom and technology contracts.

Legal 500 accredited Mr. Tavawalla as "an accomplished professional with a deep understanding of M&A transactions". In addition, Mr. Tavawalla has significant expertise in joint ventures, asset acquisitions and business transfers with a special focus on public private partnerships.

Mr. Tavawalla lead the team for the research paper titled 'Cloud Computing - Risk/Challenges: Legal & Tax Issues'.

Mr. Tavawalla is a member of the International Bar Association (IBA) along with being a member of the Intellectual Property and Technology committee of the IBA.

Email:
huzefa.tavawalla@nishithdesai.com

Scroll to Top

which is capable of identifying a person such as mobile number, address, name etc) as opposed to only SPDI which is protected under Section 43a. As per this Section, liability (imprisonment and monetary) could arise for failure to protect personal information caused by breach of a lawful contract resulting in a wrongful loss to the aggrieved person.

3. Overview of the Rules

3.1 Collection of SPDI

While collecting SPDI, explicit written consent must be obtained from the data subject by letter,, fax or email or consent given by any mode of electronic communication in relation to the purpose for which the SPDI may be used. The data subject must also be given an option to withdraw such consent and must have knowledge of and/or be provided information as to:

- the fact that information is being collected;
- the purpose for which it is being collected;
- intended recipients of the information; and
- the name and address of the agency that is collecting and/or retaining the information.

3.2 Disclosure and Transfer of SPDI

Disclosure of SPDI to a third party requires prior written approval of the data subject unless such disclosure has been agreed to in the contract between the collector and the data subject. The exception being –

- where the disclosure is necessary to be in compliance with law; or
- where the disclosure is necessary for government agencies mandated under law to procure such information.

Further, the party to whom SPDI is being disclosed shall not disclose it further.

With respect to transfer, this is only allowed if:

1. it is necessary for the performance of the lawful contract between the collector and the data subject; or
2. where the data subject has consented to data transfer.

Subject to these conditions, SPDI may be transferred to any third party that ensures the same level of data protection that is adhered to by the collector of the SPDI.

3.3 Other Obligations under the Rules

a) **Privacy Policy** – The entity itself or any other entity which is acting on behalf of such entity which collects, store, deals, or handles SPDI, is required to have a privacy policy which includes the details required under the Rules. The privacy policy should be available for review by data subjects on the website.

b) **Reasonable Security Practices** – The IT Act defines such reasonable security practices and procedures to mean security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment. Such measures may be specified in an agreement between the parties or as may be specified in any law and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Government.

Under the Rules, the Government has prescribed the international Standard IS/ISO/IEC 27001 on 'Information Technology - Security Techniques - Information Security Management System - Requirements' as a reasonable security standard.

4. Other Legislation

In addition to the IT Act, banking secrecy laws in India clearly outline the obligation of maintaining secrecy and confidentiality of customer data. The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983 specifically contains provisions which prevent such public financial institutions from divulging any information relating to the affairs of its clients. Similarly, the Banking Regulation Act, 1949 and its associated regulations and norms give due regard to the privacy principles of regulating collection, retention and security of customer data. The Credit Information Companies (Regulation) Act, 2005 gives, perhaps, the most comprehensive coverage of principles of privacy, regulating:

- access to data,
- data collection and purpose limitation,
- disclosure norms,
- obligation to maintain confidentiality, accuracy, fidelity and secrecy of the data, and
- data retention policy

both in the Act's provisions as well as in notified regulations (Credit Information Companies Regulations, 2006).

Other legislation, such as the Bankers' Book Evidence Act, 1891, the Insurance Regulatory and Development Authority Act, 1999, the Prevention of Money Laundering Act, 2002 and the Indian Income Tax Act, 1961 also have various provisions that deal with data privacy.

5. Codes of Conduct

The Banking Codes and Standards Board of India ('**BCSBI**') is a voluntary, independent and autonomous body, which sets forth rules and code of conduct for banking operations in India. These codes also focus on privacy and confidentiality of customers' information and contain *inter alia*, provisions such as:

• Confidentiality of the data to be maintained even after the customer has severed relationship with the bank except when:

- Information is required by law or is required by the banking regulator.

- There is a duty towards the public to reveal the information.
- The bank's interests require them to give the information (for example, to prevent fraud), but not for marketing purposes (unless specifically authorised by the customer)
- The bank has the customer's authorisation to reveal the information, or to give a banker's reference about the customer.

Similar codes of conduct exist for other financial services providers. The Indian Banks Association Fair Practice Code for Credit Card Operation contains similar provisions regarding confidentiality of account details of customers.

While these codes are binding on their members their actual implementation as well as the ability to enforce compliance remains a challenge.

Reserve Bank of India Guidelines

Following the final report of the Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds (better known as the G. Gopalakrishna Working Group or GGWG), the Reserve Bank of India ('**RBI**') in April 2011 issued the Guidelines on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds which is a comprehensive set of recommendations to be implemented by banks in order to ensure better information security and protection against cyber frauds.

6. Conclusion

The pace with which financial services are being remodelled to appeal to younger and newer customers has made compliance with the existing regulations extremely difficult, since data is being collected, received, possessed, stored, dealt or handled at multiple levels. This issue is further compounded by financial institutions increasingly outsourcing non-core functions to third parties.

Also, the rate of development of technology is making the application of existing laws increasingly challenging. For example, when the Rules were enacted usage of financial services via mobile phone applications was not very prevalent, however, in a short span of time this has become a major source of collection of SPDI. Therefore, the real challenge for Indian privacy legislation is to try and keep up with the changing technology and ensure that it keeps on evolving to remain relevant in the face of new challenges thrown up by technology.

In the broader Indian context, while comprehensive privacy legislation is still awaited, the Government has taken some positive steps in this regard, including setting up of a committee of a group of experts on privacy, headed by a former high court judge, to examine the state of privacy laws in India and to give their recommendations for future privacy legislation. In October 2012, this Group submitted its report[1] which examined in detail the constitutional relevance of the right to privacy in India, privacy legislation in foreign jurisdictions, the limitations and shortcomings of the current privacy framework and its recommendations in this respect. We are hopeful of comprehensive legislation being enacted on this soon.

The views and opinions expressed in this article are those of the authors alone and do not necessarily reflect the views of Nishith Desai Associates.