Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia

Harman Preet Singh
Department of Management and Information Systems, College of Business Administration
University of Hail, Saudi Arabia
mailtoharman@yahoo.com

Abstract:
Developing an effective data protection and privacy framework is vital for the progress of a country. This is because of the trend among organizations to increasingly collect personal and sensitive information. India has been recognized as the outsourcing hub by countries like UK and US. These countries consider data protection privacy and protection as fundamental right of their citizens. So, it is important for India to have robust data protection and privacy legal-policy framework to maintain its competitive position. In this paper, it has been found that India is doing better than China for data protection and privacy, but lags behind Australia. India needs to develop data protection and privacy law, as well as develop pertinent enforcement mechanisms.

Keywords: Cyber contraventions, cyber offences, data protection, privacy, Information Technology Act 2000,

1. Introduction

In many countries across the globe, the enthusiasm towards data protection policies and laws is increasing. This is because increasingly sensitive and personal data is collected by organizations. Therefore, it is important for organizations to safeguard and manage personal information. Some of the countries have already implemented robust data protection laws while some are moving in that direction. Recently, an apprehension in India has emerged regarding the influence of data protection laws passed in other countries. According to Forrester Research (2013), China has effectively no restrictions to privacy and data protection, India has minimal restrictions and Australia has some restrictions. So, a comparative study of the three countries would give some ideas for India to move forward.

2. Objectives of Study

The objectives of this research paper are presented below:

- To understand the legal as well as policy aspects of data protection and privacy in India.
- To compare the data protection and privacy policies as well as laws of India with China and Australia.
- To examine the importance of data protection and privacy for India.

3. Overview of the Laws and Policies of Data Protection and Privacy

The overview of laws and policies of data protection and privacy laws and policies in India, China and Australia is presented below:

A. Laws and Policies of Data Protection and Privacy in India

India has not passed a data protection law, unlike European Union or USA. Due to the lack of specific law, data protection in India is realized by the implementation of privacy and property rights. Privacy rights are enshrined in Constitution of India and also covered in the Information Technology Act, 2000. The property rights are covered by Indian Contract Act, 1872; the Copyright Act, 1957; and the Indian Penal Code, 1860. India's Ministry of Communication and Information Technology adopted Privacy rules, called the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (Lok Sabha Secretariat, 2013). These rules necessitate business entities to gather, process, and accumulate personal data. The personal data includes sensitive personal information to fulfill the laid down procedures (Dla Piper, 2014a).

B. Laws and Policies of Data Protection and Privacy in China

China has not passed a wide-ranging data protection legislation. So, the provisions of data protection and privacy originate from multitude of laws and regulations. China has effective pronouncements that form the basis of data protection. Examples include:

- Decision on Strengthening Online Information Protection passed in December 2012
- National Standard of Information Security Technology passed in February 2013

These pronouncements intend to protect information security; defend the interests and legal rights of citizens, legal bodies and other organizations; and guard public interest and national security. It is noteworthy that in China, the decision has same effect as the law. In addition, there are some provisions in various legal instruments that covers certain aspects of privacy and data protection, such as, Article 253 of the Criminal Law, provisions on Telecommunication and Internet User Personal Information Protection, Consumer Rights Protection Law etc. (Dla Piper, 2014b).

C. Laws and Policies of Data Protection and Privacy in Australia

In Australia, data protection and privacy policies are the mix of federal and state governments' legislation. The Australian government Federal Privacy Act 1988 and the Principles of Privacy apply to all Commonwealth Government agencies, Australian Capital Territory Government agencies and private sector companies with a minimum annual turnover of AUD 3 million. Australian states have data protection legislations. The examples include:

- Information Privacy Act, 2014 by Australian Capital Territory
- Information Act, 2002 by Northern Territory
- Personal Information Protection Act, 2004 by Tasmania
- Privacy and Personal Information Protection Act, 1998 by New South Wales (NSW)
- Privacy and Data Protection Act, 2014 by Victoria
- Information Privacy Act, 2009 by Queensland

There are some other legislations that influence the data protection and privacy for specific data or activities. They are:

- Telecommunications Act, 1997 by Commonwealth
- National Health Act, 1953 by Commonwealth
- Health Records and Information Privacy Act, 2002 by NSW
- Health Records Act, 2001 by Victoria
- Workplace Surveillance Act, 2005 by NSW

Under Privacy Act, an organization could be individual, partnership, body corporate, unincorporated association or even a trust (Dla Piper, 2014c).

4. Status of Data Protection and Privacy Rights in India

Article 21 of Indian Constitution and related constitutional provisions on fundamental rights provide the right to privacy. Article 21 of Indian Constitution states that no person can be deprived of his or her life or personal liberty apart from the process established by the law. The Supreme Court has specified in many cases that right to privacy is contained in right to life and personal liberty (Jani, 2013).

However, constitutional rights cannot be claimed against private individuals or organizations. They can be claimed only against the state or state-owned enterprises. The Information Technology Act, 2000 contains provisions against cyber contraventions under section 43(a) to (h) and cyber offences under sections 65 to 74. The cyber contraventions comprise of gaining unlawful access and extracting data from computer systems or networks. Such contraventions can lead to civil prosecution in India. The cyber offences include interfering with computer source code, hacking with intention to damage the system, and breach of privacy and secrecy. These cyber offences lead to criminal prosecution under IT Act. The IT Act also provides penalties against these offences (The Information Technology Act, 2000).

Under the provisions of IT Act, a network service provider or an intermediary is accountable for any misuse of 3rdparty information. It is also answerable for not exercising due meticulousness to avert the crime. IT Act states in term diary as an entity that acts on behalf of another entity and receives, stores, transmits or provides service regarding an electronic message. So, an outsourcing company can be held liable as a service provider. The IT Act also has extra-territorial scope. It covers offences and contraventions done outside India. It does not matter that the person committing the offence is an Indian or a foreigner. The only requirement is that the concerned computer system or network should be located in India.

The confidentiality requirements under IT Act are restricted to officers having powers under the Act. These requirements do not cover private persons. Also, the officer is not responsible for compensating the person(s), who got some damage by the disclosure. At the same time, the penalties imposed under the provisions of the IT Act range fromINR2 hundred thousand to INR 5 hundred thousand (The Information Technology Act, 2000). Such financial penalties are insignificant as compared to the gains that can accrue to a person committing cyber-crimes.

5. Status of Data Protection and Property Rights in India

Article 300A of the Indian Constitution states that no person can be deprived of his or her property except by authority of the law. However, this right cannot be claimed against private entities. It can only be claimed against the State. At the same time, the concerned data need to be considered as a person's property to enforce this right (Singhal, 1995).

The Copyright Act, 1957 of India protects Intellectual Property (IP) rights. The IP rights are protected for artistic, dramatic, musical, literary and cinematographic works. It is interesting to note that computer databases are covered under literary works. So, the act of copying and / or distributing a computer database can lead to breach of copyright. For this breach, civil and criminal remedies under the Copyright Act, 1957can be initiated (Indian Copyright Act, 1957). However, Copyright Act does not distinguish between data protection and database protection. Data protection aims to protect the private information of individuals. Database protection intends to defend the originality and investments done for the compilation, verification and presentation of databases.

The Indian Penal Code (IPC), 1860 can also be used as an effectual tool to prevent theft of data. Under the IPC; theft, misappropriation of property, and criminal breach of trust are punishable offences. The punishments include imprisonment and fine. The offence of misappropriation of property only applies to movable property under IPC. It includes corporeal property of every description. It does not include the things that are permanently attached to the land. Since, computer databases are movable in nature. So, they can be protected under the IPC to a certain degree (Law Commission of India, 1997).

6. Comparative Study of India, China and Australia

The comparative study of legal and policy provisions on privacy and data protection of India, China and Australia are given below (Dla Piper, 2014):

A. Definition of Personal Data

- India - Any information which is related to a natural person and can identify such a person. This information can also be available to a corporate entity.
- China - Any data related with a particular individual, which can be used to identify him or her.
- Australia–Any information or opinion about an individual who is identified or is reasonably identifiable.

B. Definition of Sensitive Personal Data

- India–Sensitive personal data includes financial information; physical, physiological and mental health condition; password; history of medical records; sexual orientation; biometric information etc.
- China–Sensitive personal data includes personal information whose leakage may result in bad impact to the concerned persons. Such information includes identification number of a person, mobile phone number, race, religion, political views, genetics or fingerprints.
- Australia - Sensitive personal data includes genetic information, racial or ethnic origin, political opinions, philosophical beliefs, sexual orientation, religious beliefs, health information, criminal record, membership of a trade union etc.

C. National Data Protection Authority

- India and China–There is no such authority in both countries.
- Australia - The Privacy Commissioner acts as the National Data Protection Authority.

D. Registration

There is no registration requirement in India, China and Australia.

E. Data Protection Officers

- India - Grievance officer to be appointed by every corporate entity.
- China - No requirement. However, data controller is recommended.
- Australia - No requirement. However, data protection officer is strongly recommended.

F. Collection and Processing

- India - The corporate entity would be held responsible for damages if it fails to implement and maintain compliance with privacy rules.
- China–Before collecting personal data; there should be a precise, clear and judicious purpose available with the data controller.
- Australia - An organization must not gather personal information unless it's vital for business. It should also confirm that the personal information is judicious, accurate and up-to-date.

G. Transfer

- India - Data collector has to obtain consent of provider for any transfer of sensitive personal information.
- China - Data Controller can transfer personal information to 3rdparties under some conditions.
- Australia - Personal information can only be revealed to an organization out of Australia if it takes steps to confirm that legal provisions are met.

H. Security

- India - Corporate entity needs to maintain reasonable security practices and procedures to safeguard the sensitive personal information.
- China - Data Controller needs to take appropriate measures against unauthorized processing and accidental loss or annihilation of personal data.
- Australia - Organization must put the appropriate security measures in place.

I. Breach Notification

- India - Computer Emergency Response Team (CERT) is authorized to gather, examine and spread information on cyber incidents.
- China–There is no requirement. However, guidelines recommend prompt notification of data breach to affected data subjects.
- Australia–There is no obligation. However, guidelines recommend affected individuals & Office of Australian Information Commissioner should be notified.

J. Enforcement

- India–Failure to protect personal data attracts civil and criminal penalties. Civil penalties are prescribed of up to EUR 694,450. Criminal penalties are prescribed up to 3 years imprisonment or a fine up to EUR 6950, or both.
- China - No particular consequences are there in China.
- Australia–There are fines for individuals and corporations in Australia for failing to protect personal data. For an individual, the fines are up to AUD 340,000. For corporations, the fines are up to AUD 7 million.

K. Electronic Marketing

- India - Electronic marketing is not directly addressed in India. But sending false information for causing annoyance is punishable by law.
- China -Organizations and individuals are not permitted to collect personal electronic marketing information by illegal methods.
- Australia–Electronic marketing is regulated under SPAM Act, 2003 by Commonwealth government. This act is enforced by Australian Communications and Media Authority.

L. Online Privacy

- India–There is no regulation in India regarding cookies, location data or behavioral advertising. However, IT Act contains certain provisions against civil and a criminal offence for various computer crimes.
- China - Under decision, companies are prohibited from disclosing, falsifying, damaging, selling or unlawfully providing personal electronic information to anyone else.
- Australia–The collection location data, use of cookies etc. is regulated under the Privacy Act and State and Territory privacy laws of Australia.

7. Importance of Data Protection and Privacy in India

Many developed countries have taken a lead in data protection and privacy. India has emerged as a top choice for global outsourcing (Clutch, 2015). India has clearly benefitted from outsourcing. In a survey conducted by Statistic Brain Research Institute (2015), 26% of Chief Financial Officers (CFOs) favor India for their company's outsourcing needs. The surveyed companies have cited economic, political, and cultural incentives for choosing India. Companies have also been impressed with India's pro-business and entrepreneurial climate. India's historical trade ties to the United Kingdom and United States also play an important role (George and Gaut, 2006). India also possesses low-cost and highly qualified workforce with English speaking capabilities and advance educational standards. India's steady democratic government, independent institutions, advances in Information Technology as well as convenient geography which is suitable for around the clock work makes it possible for companies to seek outsourcing to India as a preferred destination (Chandra and Narsimhan, 2005).

However, it is important to note that the global competition for outsourcing is increasing. Countries like Indonesia, Estonia, Singapore, Indonesia, Bulgaria, Philippines etc. are giving a tough competition to India. Moreover, countries in Europe and United States consider privacy a fundamental right. So, it is a need of the hour that India should toughen its data protection and privacy laws. It is also important that India should encourage the companies to self-regulate. India needs to address the loopholes in its data protection and privacy laws to address the concerns of American and European companies about their data protection and privacy. India needs to assure its outsourcing clients that cost-effectiveness of outsourcing would not be diluted by the additional costs of handling customer data privacy apprehensions, in case of a breach.

8. Conclusion

India has made the progress in data protection and privacy by putting in place various legal and policy measures. The main findings from this research regarding data protection and privacy in India are:

- Privacy and property rights conferred under the Indian legal-policy framework provides a certain amount of data protection and privacy.
- There are multitude of laws in India which protects certain aspects of data protection and privacy. These laws include the Constitution of India; Information Technology Act, 2000; Indian Contract Act, 1872; Copyright Act, 1957; and Indian Penal Code, 1860.
- India has also developed privacy rules for business entities to manage personal data.
- There is not a single comprehensive legal-policy framework in India to address data protection and privacy.
- The penalties prescribed under the existing Indian laws are not enough to deter the cyber-criminals.
- The existing Indian laws mostly applies to state- and state-owned enterprises.
- The existing Indian laws does not address finer details of data protection and privacy. For example, lack of distinction between data protection and database protection under Copyright Act, 1957.

It is clear that India has certain limitations in its data protection and privacy legal-policy framework. India seems to be doing better than countries like China, however not as good as Countries like Australia. The shortcomings of data protection and privacy in India vis-à-vis Australia are:

- India does not have a National Data Protection Authority like Privacy Commissioner in Australia.
- Unlike SPAN Act, 2003 of Australia; there is no legal-policy framework in India to address the data protection and privacy issues related with electronic marketing.
- Unlike Australia, there are no laws and regulations in India to manage cookies, location data or behavioral advertising.

A comprehensive legal policy framework to address data protection and privacy issues is need of the hour in India. Such legal and policy framework can be vital to sustain investor confidence. This is especially true for foreign investors, which send large volume of data to India for managing their back-office operations. Data protection can play an important role in outsourcing arrangements. These arrangements delegate an Indian company with a foreign company's confidential customer data, trade secrets etc. Since, outsourcing by foreign companies' plays a significant role in contributing to the Indian economy. So, it acts as an added incentive for India to strengthen its legal-policy framework to address its data protection and privacy concerns.

REFERENCES

[1] Clutch (2015). Top Outsourcing countries. URL: https://clutch.co/top-outsourcing-countries (Last accessed on: 2nd December 2018)

[2] Dla Piper (2014). Data Protection Laws of the World. pp. 20-24. URL: http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all (Last accessed on: 4th December 2018)

[3] Dla Piper (2014a). Data Protection Laws of the World. pp. 20-24. URL:

http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all (Last accessed on: 5th December 2018)

[4] Dla Piper (2014b), Data Protection Laws of the World. pp. 160-164. URL: http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all (Last accessed on: 6th December 2018)

[5] Dla Piper (2014c). Data Protection Laws of the World. pp. 69-74. URL: http://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw/functions/export.pdf?country=all (Last accessed on: 7th December 2018)

[6] Forrester Research (2013). Privacy and Data Protection by Country. URL: http://heatmap.forrestertools.com/ (Last accessed on: 7th December 2018)

[7] George, B.C. and Gaut, D.R. (2006). Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing. URL: http://blj.ucdavis.edu/archives/vol-6-no-2/offshore-outsourcing-to-india.html (Last accessed on: 7th December 2018)

[8] Indian Copyright Act (1957). URL: http://copyright.gov.in/documents/copyrightrules1957.pdf (Last accessed on: 7thNovember 2018)

[9] Jani, N. (2013). Article 21 of the Constitution of India and Right to Livelihood. Voice of Research, Volume 2, Issue 2, September 2013, ISSN No. 2277-7733.

[10] Law Commission of India (1997). One Hundred Fifty-Sixth Report on The Indian Penal Code, Volume II, August 1997. URL: http://lawcommissionofindia.nic.in/101-169/Report156Vol2.pdf (Last accessed on: 27th November 2018)

[11] Lok Sabha Secretariat (2013). Committee on Subordinate Legislation, 31st Report. Presented on 21.03.2013. Fifteenth Lok Sabha, New Delhi. URL: http://www.prsindia.org/uploads/media/IT%20Rules/IT%20Rules%20Subordinate%20committee%20Report.pdf (Last accessed on: 18th November 2018)

[12] Chandra,P. andNarasimhan,G. (2005), Nanotechnology in India: Government Support. Market Acceptance and Patent Profile. 2 Nanotechnology Law and Business, pp. 289–90.

[13] Singhal, M.L. (1995). URL: http://ijtr.nic.in/articles/art41.pdf (Last accessed on: 21st November 2018)

[14] Statistic Brian Research Institute (2015). Job Oversees Outsourcing Statistics. URL: http://www.statisticbrain.com/outsourcing-statistics-by-country/ (Last accessed on: 28th November 2018)

[15] The Information Technology Act (2000). The Gazette of India. URL: http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf (Last accessed on: 30thNovember 2018)