Telecom Business Review
13 (1) 2020, 36-46
http://publishingindia.com/tbr/

Data Protection Framework for India

Alok Shankar Pandey*, Nisheeth Dixit, Mahim Sagar*****

**Research Scholar, IIT Delhi, India. Email: alokshankarpandey@gmail.com*

***Research Scholar, IIT Delhi, India. Email: nisheethdixit@yahoo.co.in*

****Professor, Department of Management Studies, IIT Delhi, India. Email: mahimsagar@gmail.com*

Abstract

Technology has rapidly altered the course of lives of the common people and has made life fundamentally connected. People are using the digitally connected world for a plethora of activities starting from Personal Communications to Business Transactions. Activities over the internet invariably involve exchange/sharing of Data/Information. The information exchanged can provide powerful insight into the user's individual, social, political, economic interest and preferences (Nawrot et al., 2010). This information exchange resulting in collection of Data from Data Subjects is happening in a continuous manner across digital infrastructure and by almost all stake holders. This poses serious issues related to data protection and privacy of the users. Countries across the world have awakened to the need for protecting privacy and data of its citizens. India, an emerging economy, house to a sixth of global population and an aspiring Regional Power has also made numerous piecemeal efforts, mostly reactive, to address the issues of Digital Privacy and Data Protection. In this paper, the authors analyse the global practices on Data Protection with an aim to identify key ingredients which must essentially be incorporated in the Data Protection Framework formulated by India.

Keywords: Data Protection, Digital Privacy, India, GDPR

1. Introduction

Emergence of Digital delivery of Services and its absorption by the State/Public Sector and the Private Sector has led to a huge increase in digital transactions/services. Reports indicate that approximately 2.5 quintillion (IBM, 2017) bytes of data are being generated daily globally. Driven by the desire of market dominance and offering of customized yet differentiated services, Service Providers are increasingly focusing on acquisition, storage, processing, analytics and subsequent trading of data of its users. While some of the data collected is generic, a significantly large portion of this data can be classified as Personal Data or Information, some of which Sensitive and containing Personal Identifying Information (PII). Uncontrolled monetization potential of this data in the absence of comprehensive framework on the methodology of collection, retention, processing and sharing of data has its impact on privacy, identity, reputation and critical personal and financial data of the users. Breach or compromise of this data can cause irreparable harm to these users. Data has also emerged as a powerful socio, economic, political and strategic asset. The exploitation of Facebook data by Cambridge Analytica (Boldyreva, 2018) to influence political decision making and opinion shaping of citizens across various countries is a small example of how multiple data sources can be collected, collated and analyzed for targeted campaigns. Countries across the world have awakened to the value of data and the need to provide an effective data protection framework in respect of both personal and business data.

2. Literature Review

The need for a Data Protection Framework has its origins in the emerging strategic nature of Data. Countries across the world are now alive to the need for Data Sovereignty. The authors felt it was only prudent to study the initiatives and enactments by Developed and Developing countries of significance to propose a Data Protection Framework for India. The initiative by EU, that is the General Data Protection Regulations (GDPR) (Intersoft Consulting, 2016), by the BRICS countries, i.e., Brazil's Civil Rights Framework for Internet Act (Civil Internet Framework, 2014), Russia's Federal Law on Personal Data(Federation Council, 2006), China's Cyber Security Law (National People's Congress, 2018), South Africa's POPI Act (National Assembly, 2013) besides initiatives in India which include Justice AP Shah Committee (Planning Commission, 2012) and Justice BN Srikrishna Committee (MeitY, 2018), so that a balance Data Protection Framework, which is consistent with the

world community while simultaneously safeguarding India's interest, can be proposed.

3. Digital Service Delivery Model and Areas of Concern

The Non-Rivalrous, Invisible and Recombinant nature of Data (Moniodis, 2013) coupled with its growing commodification, lends it vulnerable to the possibility of uncontrolled proliferation, has the potential to harm/haunt the user, who in the first place unsuspectingly shared it with the environment, himself.

For demystifying the maze around data, a closer look at the infrastructure, stakeholders enabling delivery of digital services is essential. A typical digital service delivery infrastructure is shown in Fig. 1.

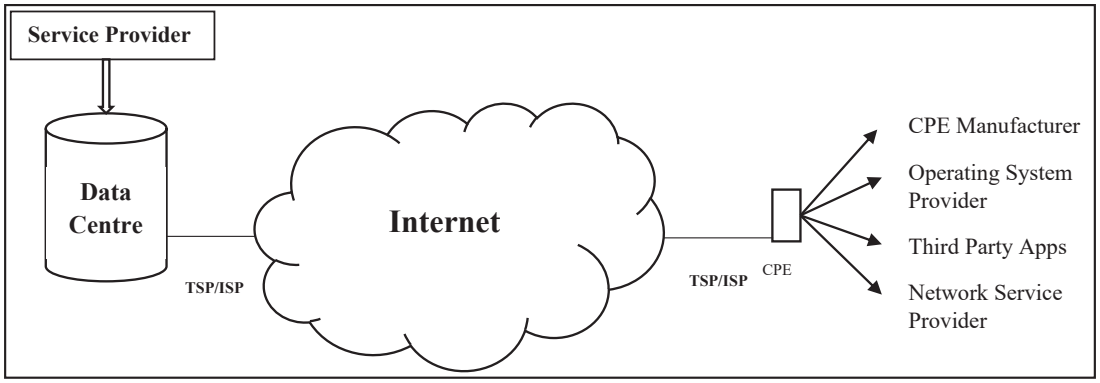


Fig. 1: Digital Service Delivery Infrastructure

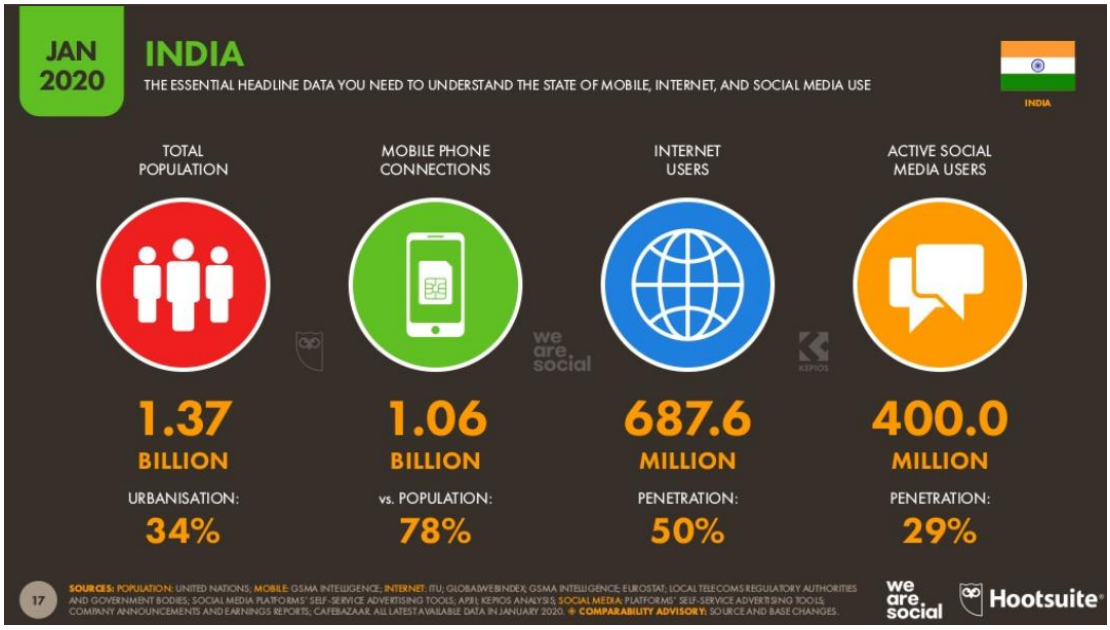
Delivery of Digital Service is now not constrained by geographical boundaries of the User's or the Service Provider's State. Typically, a Service Provider hosts the Service through a server hosted in a Data Centre. The End User, through an End User Device/Customer Premise Equipment (CPE) avails of the services over the internet. The service provisioning is based on an affirmative acceptance of the terms and conditions of provisioning of service by the Service Provider. The challenge however is that besides the User and Service Provider, there are other embedded stakeholders like the Data Centre Facility Provider, Internet/Telecom Service Provider, End User Device/CPE manufacturer and the Application Provider. Therefore, a user consent for one intended Business to Consumer (B2C) service in the digital domain creates opportunities for at many other Business to Business (B2B) and B2C services, with each stakeholder vying for a large pie of the data transmitted/shared by the User, for subsequent storage, processing, analytics and reuse. This is facilitated by obtaining a very generically worded wide sweeping one-sided consent (take it or leave it) from the user.

The consenting users are mostly unaware of the impact of sharing this seemingly harmless bits personal information, which leads to emergence of areas of concern like Information Asymmetry (TRAI, 2017), Bounded Rationality (Bhandari & Sane, 2016; Radinsky, 2015), Data Monopoly, Ownership, Integrity, Residency and Cross border Flow. Various countries across the world have therefore initiated/implemented regulatory framework for protection of data of its Data Subjects. Nearly 120 countries (Greenleaf, 2017) across the world have enacted comprehensive data protection and e-privacy laws to holistically address these issues. Various facets of Data Protection laws/initiatives by USA, OECD, EU, UK, Australia, Canada, South Africa, China, Russia, Japan, Brazil are summarized as Appendix to this paper. Analysis of the Data Protection frameworks brings out Inadequacy of Existing Regulations, Emergence of Data Protectionism and a growing realization of Citizen's Right Protection.

In light of the above it is imperative that India develop a comprehensive Data Protection Framework, for protection of its citizen's rights to data protection and privacy. In the next section we examine the existing data protection framework in India and identify key constituents which must be considered for formulating a comprehensive Data Protection Framework for India.

4. Existing State of Data Protection and Informational Privacy in India

India has embarked itself on an ambitious plan for e-governance and digitized service delivery to its citizens through the Digital India initiative (Ministry of Electronics & Information Technology, 2015). Snapshot of the present state of exploitation of Digital Infrastructure in India as on Jan 2020 is shown in Fig. 2 (Hootsuite, 2020).



Source: https://datareportal.com/reports/digital-2020-india

Fig. 2: Digital Activity in India

However, India, as on date, does not have a comprehensive Data Protection Framework. Data Protection is enabled through a combination of Constitutional Rights and Acts, Government Guidelines and Sector Specific Regulations like Privacy Law enshrined under article 21 of the constitution, IT Act 2000 (Ministry of Law, Justice and Company Affairs, 2000), Indian Contract Act 1872, IT Rules on sensitive personal data on information (Ministry of Communications and Information Technology, 2011) and various related sectoral regulations issued by RBI, SEBI, IRDAI, TRAI etc.

The above approach of piecemeal plugging challenges related to Data Protection suffers from inherent drawbacks. Data of a Data Subject is collected by Public and Private entities alike, however Data Subject can claim infringement of Fundamental Rights only from the State and not Corporate Bodies. Similarly, the State not being a Corporate Body remains exempted from the provisions of the IT Act 2000. Therefore, initiatives like tabling of draft Personal Data Protection Bill in 2006 and subsequent appointment of Justice AP Shah Committee (Planning Commission, 2012) to propose a comprehensive Data Protection Framework of India were undertaken. As on date a revised Draft of Data Protection Bill has been tabled in 2019.

A Nine judge Constitutional Bench of the Supreme Court of India, on 24 Aug 2017, ruled Right to Privacy as a Fundamental Right. Right to Privacy was analyzed in the context of global information-based society. The Government of India on 31 Jul 2017 constituted a committee (Ministry of Electronics & Information Technology 2017) headed by Justice BN Srikrishna to suggest a draft Data Protection Bill for India. The committee in Nov 2017 has published a white paper (Ministry of Electronics & Information Technology, 2017) seeking comments of the public and stakeholders.

5. Proposed Framework for Data Protection in India

It is only prudent that the proposed data protection framework not only benefits from the previous work but

also incorporate the additional experience gained and challenges faced in the intervening period. The authors have taken cognizance of both local and global initiatives in proposing a Data Protection Framework for India. Key facets of the proposed data protection framework are discussed in the succeeding paragraphs.

5.1. Scope of Regulations

Rules of Jurisdiction in International law state that State Jurisdictions end at its territorial boundaries unless specifically permitted under scope of bilateral/multilateral treaties (France V Turkey, 1927 ICJ). International Laws, however, under certain circumstances permits exercise of extra territorial jurisdiction. Processing of personal data of a citizen of a given state, over the internet, could easily take place across multiple jurisdictions. This clearly leads to a situation where action in one state has its impact/effect in another. The scope of Extra Territorial Jurisdiction must include processing of data originated from citizens of India.

5.2. Applicability of the Regulations

The regulations must apply equally to Natural/Juristic Citizens and Public/Private Entities with some reasonable exception for the State. The Regulations must be applied prospectively with provision for Retrospective enforcement on some previously collected data.

5.3. Notice and Consent

Consent as an enabling/validating mechanism enables protection of an individual's informational privacy (Reidenberg et al., 2015) and provides the moral backing to the Data Controller/Processor for their subsequent actions. 'Consent' to the 'Notice' forms the foundation of most data protection laws/frameworks across the world. The Notice should clearly state the Nature/Type of data being collected, the Use for which it is collected and whether or not it will be shared further with third parties. A differentiated level of consent (European Commission, 2011) must be provided, giving option to the user to restrict data controlled for one/all of the above options without being denied the Service by a Service Provider.

5.4. Purpose Specification and Use Limitation

The service provider or Data Collector/Processor must clearly specify the Purpose of data collection and provide for enforcement of Use Limitation by the User with certain exceptions for processing of data by the State for activities like law enforcement, legislations, public interest (European Commission, 2014). Besides facilitating a lawful means of data collection, this would prevent subsequent unexpected/objectionable use of user data (European Commission, 2013).

5.5 Sensitive Personal Data

The authors do not propose sub classification of data as sensitive or otherwise. Technology today is so pervasive that harmless bits of data aggregation, correlation and analysis, can depending on its use, cause more harm to an individual even if provision for direct protection for sensitive data exist. Differentiated levels of consent for different type of data as proposed earlier will aid adequate protection for data perceived sensitive by each Data Subject.

5.6 Data Storage Limitations

It is only logical that collected data where the purpose of use of the data has been achieved and the Data Subject's consent imposes further use limitation be erased. It must however be noted that with emergence of technologies like IoT, AI and Big Data, where potential use cases of data may not be known apriori, it makes sense that Data Retention be preferred over Storage Limitation. The authors on this count are at variance with many recent global regulations like the EU-GDPR and are of the opinion that that the data required to be retained should be anonymized (OECD, 2013). Technological Solutions be deployed for encryption and storage of anonymized data sets, while at rest or in transit, besides imposing legal penalties for violation/breach of data protection framework on user data.

5.7. Data Authenticity

An individual's right to access data about himself, allow determination of its correctness, lawful processing and

removal of inaccuracies, should therefore be at the core of the data protection framework. It is proposed that Individual should be accountable for correctness of shared consented data. Thereafter, it should be responsibility of the collector/processor to ensure data authenticity whether processed or otherwise. The User must have a right to demand data correction/updation.

5.8. Safeguard Against Pitfalls of Automated Decisions

Data Protection framework must provide for grant of relief against inconvenience caused to Data Subject due to application of incorrect/inaccurate logic for arriving at automated decision on user data sets. The User must have the liberty to restrict data processing based on inaccurate data which could lead to denial of services to him.

5.9. Data Portability

Data portability is very important for ensuring user autonomy and therefore is correctly being considered as an integral part of the envisaged data protection framework.

5.10. Right to be Forgotten

It is essential that an 'Exit Clause' mandatorily be incorporated in Notices enabling the Data Subject to exercise his Right to be Left Alone or Forgotten from the digital world. This directly implies that a data controller/processor must erase all data of a Data Subject on exercise of his Right to be Forgotten (Jeffries, 2011).

5.11. Data Transfer Tracking

Any Data Controller/Processor must not share data of a Data Subject with any third party without explicitly informing the Data Subject of the intention to do so and obtaining the consent of the Data Subject.

5.12. Data Protection Authority

It is important that a robust, independent and technically sound supervisory Authority, namely Data Protection Authority be established. The fact that Sectorial Regulators exist and have evolved relevant regulatory framework for their respective sectors, it may be more prudent to adopt the co-regulatory model. The Data Protection Authority could also serve as a platform for Inter Sector Regulatory Synchronization. The Data Protection Authority must undertake periodic audits of organizations to ensure that the organizations collecting/processing data are adhering to the laid down regulatory Framework.

5.13. National Perspective

It is important that a state also protects its Data Sovereignty. Economic activities in this digital age are largely data centric and therefore certain issues like Data Democracy, Data Localization and Cross Border Flow of Data should be dealt as subjects of National Strategy.

6. Conclusion

India, home to one sixth of the global population and one of the fastest growing economy, must adopt an effective yet realistic Data Protection Framework. The migratory path from the existing state of Data Colonization to the desired state of regulated Data Democracy will be very challenging. A global consensus on data protection framework and its consequent compliance by the State and Sectoral stakeholders is the most desirable state. However, since the utopian state does not exist, efforts must also be made at regional levels or between member states having common stated aim and objective towards data protection like the EU to evolve a common data protection framework.

Early finalization and adoption of a Data Protection Framework based on the factors highlighted in this paper would help India catapult itself towards a growth trajectory effectively harnessing the potential of the next generation technologies.

Appendix

Table 1: Summary of Important Provisions of Data Protection in Various Countries

Parameters	*EU*	*UK*	*US*	*Canada*	*Australia*	*South Africa*	*China*	*Russia*	*Japan*	*Brazil*
Law	EU GDPR 2018	Data Protection Act 2018	Privacy Act FTC, GLB, HIPAA, COPPA Electronic Communication Privacy Act	Privacy Act, PIPEDA	Privacy Act 1988	POPI,2013	Systems for Cyber Security Law 2018	Federal Law on Personal Data 2006	APPI 2016	Civil Rights Framework for the Internet 2014
Extra Territorial Scope	Includes controllers and processors outside EU	Applicable to Overseas Organisations and Operators which carries on business in Australia and personal data collected or held in Australia.		Silent and subject to interpretation by courts		Applies to automated or non-automated data processing within South African Territory only	All entities irrespective of physical location accessing localised Chinese data automatically covered under the Chinese law	All entities irrespective of physical location accessing localised Russian data automatically covered under the Russian law		
Applicability Of The Regulations	Natural Persons Public and Private Entities	Public and Private Entities	Some Private and Most Govt Entities	Govt and Private Entities No retrospective application	Some Private and Most Govt Entities	Natural and Juristic Persons Consensus on no retrospective application				
Notice And Consent	Explicit, Specific, Informed and Unambiguous	Explicit, Specific, Informed and Unambiguous	Consent is mandatory	Graduated consent standard Consent valid only if individual reasonably understands nature, purpose and consequence of consent	Consent not an essential prerequisite. Necessity of collection of data must exist	Explicit, Specific, Informed and Unambiguous			Consent is mandatory	Consent is mandatory

Parameters	*EU*	*UK*	*US*	*Canada*	*Australia*	*South Africa*	*China*	*Russia*	*Japan*	*Brazil*
Purpose Specification And Use Limitation	Strict adherence to purpose and use limitations agreed between Data subject and Controller/ Processor with exemption for Scientific, Historical, Statistical Research or Law Enforcement	Strict adherence to purpose and use limitations agreed between Data subject and Controller/ Processor with exemption for Scientific, Historical, Statistical Research or Law Enforcement	Strict adherence to purpose and use limitations agreed between Data subject and Controller/ Processor	Strict adherence to purpose and use limitations agreed between Data subject and Controller/Processor with exemption for Scientific, Historical, Statistical Research or Law Enforcement	Adherence to purpose specification for data collection is expected. Consent required for secondary use with exemptions for law enforcement	Strict adherence to purpose and use limitations agreed between Data subject and Controller/Processor Only compatible further processing permitted			Strict adherence to purpose and use limitations agreed between Data subject and Controller/Processor	Strict adherence to purpose and use limitations agreed between Data subject and Controller/Processor
Data Storage Limitations	Storage limited to purpose of use or archiving for research purposes	Storage limited to purpose of use	Data no longer required after purpose of use is over must be destroyed. Exemption for data required for legal purposes	Data no longer required after purpose of use is over must be destroyed or anonymised	Data no longer required after purpose of use is over must be destroyed. Exemption for data required for legal purposes	Storage limited to purpose of use or archiving for contract verification and research purposes				
Data Authenticity	Accuracy of Data be ensured through updation and rectification or erasure of inaccurate data	Accuracy of Data be ensured through updation and rectification of inaccurate data	Accuracy of Data be ensured through updation and rectification of inaccurate data	Accuracy of Data be ensured through rectification of inaccurate data. Updation permitted only if required for processing within the specified purpose of use	Accuracy of Data be ensured through updation and rectification of inaccurate data	Accuracy of Data be ensured through updation and rectification of inaccurate data			Accuracy of Data be ensured through updation and rectification of inaccurate data	Accuracy of Data be ensured through updation and rectification of inaccurate data

Parameters	*EU*	*UK*	*US*	*Canada*	*Australia*	*South Africa*	*China*	*Russia*	*Japan*	*Brazil*
Safeguard Against Pitfalls Of Automated Decisions	Data Subject has right to know the details of Data Processor, Access and update personal data, verify purpose of use and logic behind automated decision	Data Subject has right to access and update personal data, verify purpose of use and logic behind automated decision		Data Subject has right to access challenge accuracy, completeness of data, update personal data and verify purpose of use. Exemption include non updation if updation/ correction cost is prohibitively costly etc	Data Subject has right to access personal data. This right is not absolute and can be denied under exempted circumstances. Data updation requests can be made for correction of inaccurate data	Data Subject has right to know the details of Data Processor, Access and update personal data, verify purpose of use and details of data required to de destroyed/ deleted. Exemption stipulated by "Promotion of Access to Information Act 2000".				
Restriction And Objection To Processing	Specific to EU or countries following EU model, not translated into law	Broadly following EU model, not translated into law				Broadly following EU model, not translated into law				Broadly following EU model, not translated into law
Data Portability	Specific to EU or countries following EU model, not translated into law	Broadly following EU model, not translated into law				Broadly following EU model, not translated into law				Broadly following EU model, not translated into law
Right To Be Forgotten	Recognised by GDPR	Recognised by DPA 2018		Upheld under PIPEDA		Not explicitly permitted but caters requests for deletion of personal data				Upheld under the Civil Rights Framework

Parameters	*EU*	*UK*	*US*	*Canada*	*Australia*	*South Africa*	*China*	*Russia*	*Japan*	*Brazil*
Data Transfer Tracking										
Data Localisation	Data to be localised within EU				Restrictions imposed on transfer of certain types of data outside Australian territory		Data centres storing data of Chinese citizens must be located within Chinese Territory	Data centres storing data of Russian citizens must be located within Russian Territory		Data centres storing data of Brazilian citizens must be located within Brazil's Territory
Cross Border Flow of Data	Adequacy Test Model contract laws and Binding Corporate Rules	Adequacy Test Model contract laws and Binding Corporate Rules	Privacy Shield	Permitted. Organisations sharing data responsible for its protection	Automatic application of APP on recipient entity by means of extra territorial jurisdiction	Permitted if recipient country has same level of Data Protection guaranteed as existent in South Africa			Permitted if recipient country has same level of Data Protection guaranteed as existent in Japan	Permitted if recipient country has same level of Data Protection guaranteed as existent in Brazil

References

Nawrot, F., Syska, K., & Świtalski, P. (2010). Horizontal application of fundamental rights: Right to privacy on the internet. Retrieved from http://en.zpc.wpia.uw.edu.pl/wp-content/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf

IBM. (2016). 10 Key marketing trends for 2017. Ibm. Com, 18. Retrieved from ftp://ftp.www.ibm.com/software/in/pdf/10_Key_Marketing_Trends_for_2017.pdf

Boldyreva, E. L., Grishina, N. Y., Duisembina, Y., & Peter, C. (2018). 18th PCSF 2018 professional culture of the specialist of the future Cambridge analytical: Ethics and online manipulation with decision-making process. *The European Proceedings of Social & Behavioural Scienced*. Retrieved from https://doi.org/10.15405/epsbs.2018.12.02.10

Moniodis, C. P. (2013). Moving from Nixon to NASA: Privacy' s second strand-a right to informational privacy. *Yale Journal of Law and Technology Article*, *15*. Retrieved from https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1080&context=yjolt

TRAI. (2017). Privacy, security and ownership of the data in the telecom sector. Retrieved from https://www.trai.gov.in/sites/default/files/Consultation_Paper%20_on_Privacy_Security_ownership_of_data_09082017.pdf

Bhandari, V., & Sane, R. (2016). Towards a privacy framework for India in the age of the internet. Retrieved from https://macrofinance.nipfp.org.in/PDF/BhandariSane2016_privacy.pdf

Radinsky, K. (2015, March). Data monopolists like google are threatening the economy. HBR. Retrieved from https://hbr.org/2015/03/data-monopolists-like-google-are-threatening-the-economy

Graham, G. (2017, January 30). *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*. 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 17-45. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

MeitY. (2015). Digital India. Retrieved from https://digitalindia.gov.in/

We are Social. (2018). Digital in 2018 in Southern Asia. Slide 69. Retrieved from https://www.slideshare.net/wearesocial/digital-in-2018-in-southern-asia-86866282

Department of Telecommunications. (2000). Information technology act, 2000. Retrieved from https://dot.gov.in/sites/default/files/itbill2000_0.pdf?download=1

MeitY. (2011). IT Rules 2011. Retrieved from https://www.wipo.int/edocs/lexdocs/laws/en/in/in099en.pdf

Planning Commission-Government of India. (2012). Report of the group of experts on privacy government of India planning commission. Retrieved from https://www.dsci.in/sites/default/files/documents/resource_centre/Report of the Group of Experts on Privacy constituted by Planning Commission of India.pdf

MeitY. (2017). Constitution of a committee of experts to deliberate on a data protection framework for India. Retrieved from https://www.meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf

MeitY. (2017). White paper of the committee of experts on a data protection framework for India. Retrieved from https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf

Publications of the Permanent Court of International Justice. (1927). Case of S.S. Lotus (France v. Turkey). Retrieved from https://www.icj-cij.org/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf

Reidenberg, J. R., Russel, N. C., Callen, A. J., Qasir, S., & Norton, T. B. (2014). Privacy harms and the effectiveness of the notice and choice framework. *A Journal of Law and Policy for the Information Society, 11*(2). Retrieved from https://kb.osu.edu/bitstream/handle/1811/75473/ISJLP_V11N2_485.pdf?sequence=1

European Commission. (2011). Article 29 data protection working party opinion 15/2011 on the definition of consent. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

European Commission. (2014). Article 29 data protection working party. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

European Commission. (2013). Article 29 data protection working party opinion 03/2013 on purpose limitation. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

OECD. (2013). OECD guidelines on the protection of privacy and transborder flows of personal data. Retrieved from http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

The Guardian. (2011). Why we must remember to delete – and forget – in the digital age. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2011/jun/30/remember-delete-forget-digital-age

MeitY. (2018). A free and fair digital economy protecting privacy, empowering Indians. Retrieved from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

Intersoft Consulting. (2016). General data protection regulation (GDPR). Retrieved from https://gdpr-info.eu/

Chamber of Deputies. (2014). Brazilian civil framework for the internet. Retrieved from https://bd.camara.leg.br/bd/bitstream/handle/bdcamara/26819/bazilian_framework_ internet.pdf?sequence=1&isAllowed=y

Russian Federation. (2006). Russian federation legislation in the field of personal data. Retrieved from https://iapp.org/media/pdf/knowledge_center/Russian_Federal_Law_on_Personal_Data.pdf

Republic of South Africa. (2013). Government gazette. Retrieved from https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf

KPMG. (2017). Overview of China's cybersecurity law. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf