DATA PROTECTION ON CYBERSPACE - ISSUES AND CONCERN

DISSERATION FOR

POST GRADUATE DIPLOMA

IN

CYBER LAWS AND CYBER FORENSICS

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY, BANGALORE

Mehul Kothari

STUDENT ENROLLED IN

POST GRADUATE DIPLOMA IN

CYBER LAWS AND CYBER FORENSICS

TABLE OF CONTENTS

TABLE OF CASES

TABLE OF STATUTES

1. Information Technology Act of 2000

2. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act)

3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

ABBREVIATIONS

1. **APEC** - Asia Pacific Economic Cooperation Privacy Framework
2. **APIs** - Application Programming Interfaces
3. **BCR** - Binding Corporate Rules
4. **BPL -** Below Poverty Line
5. **CBPR** - Cross-Border Privacy Rules System
6. **CDPA** - The Copyright, Designs and Patents Act, 1988
7. **COPPA** - Children's Online Privacy Protection Act
8. **CSS –** Cyberspace, Security, and Safety
9. **DDA** - Developer Distribution Agreement
10. **DIT** - Department of Information Technology
11. **DSCI** - Data Security Council of India
12. **EDF** - Electronic Development Fund
13. **ESDM** - Electronics System Design and Manufacturing
14. **EU** - EUROPEAN UNION
15. **FTC Act** - Federal Trade Commission Act
16. **GDPR** - General Data Protection Regulation
17. **GIS** - Geographic Information Systems
18. **HDFS** - Hadoop Distributed File System
19. **HIPAA** - The Health Insurance Portability and Accountability Act
20. **ICANN** - Internet Corporation for Assigned Names and Numbers
21. **IGF** - Internet Governance Forum
22. **IMDb** - Internet Movie Database
23. **IoT** - Internet of Things
24. **ISPs**- Internet Service Providers
25. **IT Act** - Information Technology Act of 2000
26. **ITU** - International Telecommunications Union
27. **MNCs -** Multi-National Corporates
28. **NOFN** - National Optical Fibre Network
29. **NeGP** - National e-Governance Plan
30. **NETmundial** - Global Multistakeholder Meeting on the Future of Internet Governance

31. **OLAP** - Online Analytical Processing
32. **OS** - Operating System
33. **PII -** Personal Identifiable Information
34. **POPI Act** - Protection of Personal Information Act, 2013
35. **SPDI** - Sensitive Personal Data of Information
36. **UIDAI -** Unique Identification Authority of India
37. **UNCITRAL** - United Nations Commission on International Trade Law
38. **UOI** - Union of India
39. **U.S.A** - Unites States of America
40. **WWW –** World Wide Web

1. INTRODUCTION

In this era of development, the first world economies have made a transition from industrial based economies to information-based economies. This is the consequence of a burst in information being disseminated by all users and the means by which it is being disseminated that is resulting in far-reaching technological developments. Today, substantial investments of companies are directed towards the collection of such information, most companies are drawing up elaborate databases for their core business activities and analysing those databases to make the product more customer-relevant. Databases are playing an important role in the development of product in today's information centric market.

This has made the collection and systematic recording of such data a very lucrative business option. Though this raises concerns regarding the protection of such databases. The ever-increasing pressure to provide legislative protection for databases has arisen from the increase in harvesting of mass data available in almost every area of commerce and science, and the enhanced technological availability to transform that raw data into digital accessible databases.

Database protection applies to both electronic and non-electronic databases. Database protection is a priority policy agenda on most world economies plan to address the issues concerning the transfer of databases with such ease (along with other sensitive information) which has ironically increased the unauthorised access to these databases. The technological advances allow database of information to be connected together and allowing even greater quantities of data to be processed, which in turn is creating a challenge for regulation given the transnational nature of the internet. Despite the emergence of international practice

standards for data protection, there is still progress to made towards the harmonisation of such laws.

Data privacy is defined as the appropriate use of data, when multi-national corporates (MNCs) access data on permission and collect the required information which is provided by the users or entrusted to MNCs on consent basis by users. The data is used in accordance with the underlying agreed agreements. Data security is referred to as the confidentiality, availability and integrity of data, to ensure that data is not being used or accessed by unauthorized individuals or parties, and also ensuring that data is available to those with the authorized access.

There are certain elements which are significant to cover data protection policies in cyberspace which include (a) Data security accountability, means the various types of data that should be classified under distinguished categories and management made aware of the responsibility in sharing each classified type of data and whether or not access is authorized; (b) Policies that govern network services, issues such as remote access, configuration of IP addresses on systems that the company uses, security of components like routers and servers, and detecting cases of network intrusion; (c) scanning for vulnerabilities, meaning the corporates should have a routines procedure to check the networks regularly; (d) Acceptable use, meaning the employees should be aware about the responsibility with which they access the company's network & servers; (e) Monitoring Compliance, meaning have regular audits, check and balances in place to ensure that the data security policy is intact; and (f) Monitoring and control.

2. MEANING OF DATABASE

Database systems are an essential component of life in modern society, most of us encounter several activities every day that involve some interaction with a database. For example, if we go to the bank to deposit or withdraw funds, if we make a hotel or airline reservation, if we access a computerized library catalogue to search for a bibliographic item, or if we purchase something online – such as a book, toy, or computers – chances are that our activities will involve someone or some computer program accessing a database and storing and saving that relevant information.[1] These daily interactions are examples of what we call as database applications, in which information is stored and accessed in either textual or numeric manner.

Database is a collection which allows selection and arrangement of data by attributes that are classified in the database. The Copyright, Designs and Patents Act, 1988 (CDPA) (UK Act) defines a database as: "A collection of independent works, data or other materials which: (a) are arranged in a systematic or methodical way; and (b) are individually accessible by electronic or other means"[2]

Furthermore, database is defined in Article 1 (2) of the European Union Directive on Legal Protection of Databases as a collection of independent

[1] Fundamentals of Database System by Ramez Elmasri, Shamkant B. Navathe Published by Addison-Wesley, Pearson [Chapter 1 – Database and Database Users; Page 3]

[2] Section 3A, Copyright, Designs, and Patents Act, 1998 (CDPA) (as amended by regulations)

works, data or other materials arranged in a systematic or methodical way and capable of being individually accessed by electronic or other means.[3]

A database, or information system contains two primary forms of digital property (i) raw data, which is a source of knowledge or entertainment value; (ii) tools, which are programs that can be used to communicate, store, or manipulate raw data. A developed database is an interrelated set of collection, processing, merger, storage, or dissemination of data.[4]

In the past few years, advancements in technology have led to exciting new applications of database systems, the technology has made it possible to store such data digitally and become an important component of multimedia databases. The uses of database in different segments of work are explained[5]: (a) Geographic information systems (GIS) can store and analyse maps, weather data, and satellite images. (b) Data warehouses and online analytical processing (OLAP) systems are used in many companies to extract and analyse useful business information from very large databases to support decision making. (c) Real-time and active database technology is used to control industrial and manufacturing processes. (d) Database search techniques are being applied to the World Wide Web (WWW) to improve the search for information that is needed by users browsing the Internet.

3. CYBER SPACE

[3] Council Directive 96/9, March 11, 1996 O.J. (L 77) 20 (EC) (Jan. 29, 2011) http://europa.eu.int/ISPO/infosoc/legreg/docs/969ec.html; W.K. Khong, National and International Developments on Copyright and Rights in Databases 6 MALYSIAN J. LIB & INFO. SCIENCE 71, 72 (2001)

[4] Brown Mart, Bryan Robert M & Conley John M, Database Protection in a Digital World, Richmond Journal of Law & Technology, 6 (1) (1992) Pg. 2-10

[5] Fundamentals of Database System by Ramez Elmasri, Shamkant B. Navathe Published by Addison-Wesley, Pearson [Chapter 1 – Database and Database Users; Page 3]

The domains of cyberspace are bifurcated into three parts i.e. **(a)** System domain which comprises of technical foundation, infrastructure, and architecture of cyberspace. It includes hardware and software, as well as the infrastructure items supporting them, such as the electrical power grid. **(b)** Content and application domain contains both the information base that resides in cyberspace and the mechanism for accessing and processing this information. **(c)** Governance domain overlays all of the aspect of cyberspace, including the technological specifications for the systems domain, the conventions for the data formatting and exchanges in the content and application domain. [6]

The system domain of cyberspace is the infrastructure that carries, stores and manipulates information. A major portion of the modern economy is associated with manufacturing the components and systems of cyberspace, including computer chips, desktop computers, routers, servers and operating systems. Another major component of the economy is associated with operating this infrastructure, including Internet service providers (ISPs), telecommunications firms, electrical power companies, and other organizations. [7]

The content and application domain of cyberspace provides the technical underpinnings of the network, but it is merely an infrastructure on which data can be stored, transmitted, and content can be manipulated or information used by various software applications is accessible.[8]

[6] Introduction to the Structural Elements of Cyberspace by Elihu Zimet and Edward Skoudis [Chapter 4] Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-04.pdf
[7] Ibid
[8] Ibid

With every evolving activity of individual, organizations, and nations conducted in cyberspace, the security of these transactions and activities proves as an emerging challenge for society. The security gaps in computer and telecommunications structures allows these arrangements to be subject to adverse or hostile actions. In addition to deliberate threats, information systems operating in cyberspace can fall prey to unforeseen events due to intervention of bad actors i.e. hackers, zealots or disgruntled insiders, to satisfy personal agendas; criminals, for personal financial gain; terrorists or other malevolent groups, to advance their cause; commercial organizations, for industrial espionage or to disrupt competitors; nations, for espionage or economic advantage or as a tool of warfare[9], that result in unintended situations.

In the new cyberspace world, government, business, individuals, and society as a whole require a comprehensive program of cyberspace, security, and safety (CSS).

The governance of cyberspace is complex and contested, due to the decentralized nature of the medium of delivery, largely owned and operated by private sector, consequently creates an interest for governments and civil society and poses a threat to traditional form of governance. The question that arises in our mind is that due to its transnational nature, who should be involved in cyber governance. Internet governance scholar Laura DeNardis describes multi-stake in cyberspace as "a constantly shifting balance of powers between private industry, international technical governance institutions, governments and civil society."[10] The multiple stakes in the governance of cyberspace does not envision all parties to be involved in the same manner and in same degree in all matters but to have distinguished roles to play. For

[9] Emerging Challenge: Security and Safety in Cyberspace by Richard O Hundley and Robert H Anderson Published by RAND Corporation (1997)
[10] Laura DeNardis, The Global War for Internet Governance (New Haven and London: Yale University Press, 2014) 227

example, technical matters related to the smooth operation of cyberspace should be largely handled by the private sector, as the private sector are responsible for distributed databases across cyberspace, so the technical know how of the subject would be best suited to the private sectors to deal in scenarios where an issue arises. While, the states can be party to international treaties or have nationalised legislation for regulating cyberspace.[11]

CYBER GOVERNANCE

The contemporary cyber governance encompasses several governance processes, including the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunications Union (ITU), and Internet Governance Forum (IGF), and the Global Multistakeholder Meeting on the Future of Internet Governance (NETmundial). Each of these institutes have its unique strengths and weakness, while all require improvement to be effective.[12]

ICANN is a private, non-profit organization, which performs key technical tasks to ensure the smooth functioning of the internet. In theory, ICANN takes a community-based, consensus driven approach to policymaking through open discussion of its policies.[13]

ITU is a specialized UN body for information and communication technologies that allocate global radio spectrum and satellites which orbit

[11] Policy Brief - Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance by The Hague Institute for Global Justice [November 2015] – Who should govern cyberspace? An analysis of multi-stakeholder governance. [Page 4]
[12] Ibid [Multistakeholder models of cyber governance: Strengths and weaknesses; Page 6]
[13] Ibid

the world and develop technical standards.[14] The Least Developed Countries, which primarily engage in cyber governance through the ITU, often see it as "the most appropriate forum for governing global electronic networks, including the Internet."[15]

IGF, created by World Summit on the Information Society in 2006, brings together diverse stakeholders to annual meetings about public policy issues pertaining to the Internet under the aegis of the UN.[16]

NETmundial, is widely considered to have been a successful process of Multistakeholder engagement on cyber governance issues. Following revelations of large-scale data surveillance undertaken by the US National Security Agency, the Brazilian government initiated NETmundial, which brought together four groups of stakeholders (government, the private sector, civil society and the academic technical community) in quasi-equal numbers, with three levels of participation: content submissions through an online platform: online public comments on a draft of the outcome statement; and open-microphone session for participants to directly address the plenary. In addition, the drafting sessions took place in the public eye, making them more transparent. NETmundial Multistakeholder Statement was released after two days of deliberation involving over 900 participants and reinforced the concept of multistakeholderism[17], stating that "Internet governance should be built on democratic, multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders. The respective roles and responsibilities of stakeholders

[14] Ibid
[15] Enrico Calandro and Nicolo Zingales, "Stakeholders' involvement and participation in the Internet governance ecosystem from an African perspective," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015)
[16] Policy Brief - Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance by The Hague Institute for Global Justice [November 2015] [Multistakeholder models of cyber governance: Strengths and weaknesses; Page 6]
[17] Ibid; Page 7

should be interpreted in a flexible manner with reference to the issue under discussion.[18]

Security and Safety in Cyberspace – Inadequate

As is well known, cyberspace does not respect national boundaries. In recent years more and more nations throughout the world have become 'connected' to the world wide web, and within those nations connectivity has become more and more universal.[19]

The information processing systems and telecommunication systems currently in use throughout the world have security flaws, and new security flaws are being uncovered almost every day, usually as a result of hacking activities. As new developments and applications of information technology become available and as human activities in cyberspace continually expand, security efforts appear to be lagging behind.[20]

Cyberspace is perpetually evolving and businesses are eager to be ahead of the edge, therefore tend to adopt the new technologies, which create innumerable opportunities along with the unanticipated risks attached to them.

Since the inception of internet, technological developments are all pervading, by advancing access digitally the barrier constraint of sharing such information seems to have vanished. The primary concern of any

[18] NETmundial Multistakeholder Statement, - Global Multistakeholder Meeting on the Future of Internet Governance, accessed August 11, 2015 [http://netmundial.br/wp-content/uploads/2014/04/ NETmundial-Multistakeholder-Document.pdf]
[19] Emerging Challenge: Security and Safety in Cyberspace by Richard O Hundley and Robert H Anderson [Published by RAND Corporation 1997] Page 238
[20] Ibid; Page 239

business which attempts to conduct operations online, is the security and privacy of data shared with the said company. Data piracy is a nefarious problem due to the recent developments in information technology, as Data is an intangible asset, theft occurs when digitized confidential information has been accessed without the individual's authorization.

4. DATA PROTECTION - Right to Privacy

Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used and disclosed.[21] Article 4 (2) of the EU General Data Protection Regulation defines the word processing of personal data through automated means such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[22]

It is crucial to understand this concept in relation with privacy, as privacy can have different meanings based on the context. Three broad types of privacy have been identified: the privacy pertaining to physical spaces, bodies and things (spatial privacy); the privacy of certain significant self-defining choices (decisional privacy); and the privacy of personal information (informational privacy).[23] The concept of data protection is primarily linked with the idea of informational privacy.[24]

The word privacy has been derived from the Latin word *Privatus* which means 'separate from rest'. It can be defined as capability of an individual or group secludes themselves or information about themselves and thereby reveal themselves selectively. Privacy can be understood as a right of an individual to decide who can access the

[21] Lee Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic, and Limits' 2 (Kluwer Law International: The Hague / London / New York, 2002)
[22] Article 4 (2) of the EU General Data Protection Regulation, 2016 (Regulation (EU) 2016/679).
[23] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).
[24] Maria Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right,' 3(2) International Data Privacy Law 88 (1 May 2013).

information, when they can access the information, what information they can access.[25]

Privacy is undoubtedly, a basic human right to life. Privacy regarding information which involves most importantly the establishment of rules relating to data protection as data is a valuable asset in this era of information technology and needs to be protected through a established framework.

The recent Supreme court judgment Justice K.S. Puttaswamy (Retd.) v. Union of India[26] has established that the right to privacy is a fundamental right guaranteed to every citizen of India, under the Constitution of India. In, analysing the issues beforehand, the Constitution bench delves into multiple facets attempting to understand how privacy can be protected in each of the situations. One such facet of the decision was digital platforms, wherein each individual spends more time on the internet, exchanging sensitive information with service providers and third-party users on an interaction basis, resultant internet becoming a repository of such invaluable identifiable information of millions of users being generated and stored on internet.

The concepts of informational privacy along with data information and data privacy is dealt under Part S of the judgment.[27]

---

[25] Privacy and Data Protection in Cyberspace in Indian Environment by Shrikant Ardhapurkar, Tanu Srivastava, Swati Sharma, Mr. Vijay Chaurasiya, and Mr. Abhiskeh Vaish [International Journal of Engineering Science and Technology Vol. 2(5), 2010 Page 942-951]

[26] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others [AIR 2017 SC 4161]

[27] Ibid [Informational Privacy – Part S] Page 246

Ours is an age of information. Information is knowledge. The old adage that "knowledge is power" has stark implications for the position of the individual where data is ubiquitous, an all-encompassing presence. Technology has made life fundamentally interconnected. The internet has become all pervasive as individuals spend more and more time online each day of their lives. Individuals connect with others and use the internet as a means of communication. The internet is used to carry on business and to buy goods and services. Individuals browse the web in search of information, to send e-mails, use instant messaging services and to download movies. Online purchases have become an efficient substitute for the daily visit to the neighbouring grocery stores. Online banking has redefined relationships between bankers and customers. Online trading has created a new platform for the market in securities. Online music has refashioned the radio. Online books have opened up a new universe for the bibliophile. The old-fashioned travel agent has been rendered redundant by web portals which provide everything from restaurants to rest houses, airline tickets to art galleries, museum tickets to music shows. These are but a few of the reasons people access the internet each day of their lives. Yet every transaction of an individual user and every site that she visits, leaves electronic tracks/ footprints generally without their knowledge. These electronic tracks contain powerful means of information which provide knowledge of the sort of person that the user is and her interests.[28] Individually, these information silos may seem inconsequential. In aggregation, they disclose the nature of the personality: food habits, language, health, hobbies, sexual preferences, friendships, ways of dress and political affiliation. In aggregation,

[28] Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, "Horizontal application of fundamental rights – Right to privacy on the internet", 9th Annual European Constitutionalism Seminar (May 2010), University of Warsaw, available at http://en.zpc.wpia.uw.edu.pl/wpcontent/uploads/2010/04/9_Horizontal_Application_of_Fundamental_Rights.pdf

information provides a picture of the being: of things which matter and those that don't, of things to be disclosed and those best hidden.[29]

Popular websites install cookie files on the user's browser, these cookies can tag browsers for unique identified numbers, which allow them to recognise rapid users and secure information about online behaviour. Information, especially the browsing history of a user is utilised to create user profiles. The use of algorithms allows the creation of profiles about internet users. Automated content analysis of e-mails allows for reading of user e-mails. An e-mail can be analysed to deduce user interests and to target suitable advertisements to a user on the site of the window. The books which an individual purchase on-line provide footprints for targeted advertising of the same genre. Whether an airline ticket has been purchased on economy or business class, provides vital information about employment profile or spending capacity. Taxi rides booked on-line to shopping malls provide a profile of customer preferences. A woman who purchases pregnancy related medicines on-line would be in line to receive advertisements for baby products. Lives are open to electronic scrutiny. To put it mildly, privacy concerns are seriously an issue in the age of information.[30]

A Press Note released by the Telecom Regulatory Authority of India on 3 July, 2017[31] is indicative of the prevalence of telecom services in India as on 31 December, 2016. The total number of subscribers stood at 1151.78 million, reflecting a 11.13% change over the previous year. There were 683.14 million urban subscribers and 468.64 million rural subscribers. The total number of internet subscribers stood at 391.50 million reflecting an 18.04% change over the previous quarter. 236.09

[29] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others (AIR 2017 SC 4161) [Informational Privacy – Part S] [para 170 Page 246]
[30] Ibid [para 171; Page 248]
[31] Press Release 45/2017, available at http://trai.gov.in/sites/default/files/PR_No.45of2017.pdf

million were broadband subscribers. 370 million is the figure of wireless internet subscribers. The total internet subscribers per 100 population stood at 30.56; urban internet subscribers were 68.86 per 100 population; and rural internet subscribers being 13.08. The figures only increase.[32]

The age of information has resulted in complex issues for informational privacy. These issues arise from the nature of information itself. Information has three facets: it is nonrivalrous, invisible and recombinant[33]. Information is nonrivalrous in the sense that there can be simultaneous users of the good – use of a piece of information by one person does not make it less available to another. Secondly, invasions of data privacy are difficult to detect because they can be invisible. Information can be accessed, stored and disseminated without notice. Its ability to travel at the speed of light enhances the invisibility of access to data, "information collection can be the swiftest theft of all"[34]. Thirdly, information is recombinant in the sense that data output can be used as an input to generate more data output.[35]

Data Mining is a process that uses a variety of data analysis tools to discover knowledge, patterns and relationships in data that may be used to make valid predictions[36]. Metadata and the internet of things have the ability to redefine human existence in ways which are yet fully to be perceived. In an age of rapidly evolving technology it is impossible

---

[32] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others (AIR 2017 SC 4161) [Informational Privacy – Part S] [para 172 Page 248]
[33] Christina P. Moniodis, "Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy", Yale Journal of Law and Technology (2012), Vol. 15 (1), at Page 153
[34] Ibid
[35] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others (AIR 2017 SC 4161) [Informational Privacy – Part S] [para 173 Page 249]
[36] Use of Object-Oriented Concepts in Databases for Effective Mining by Ajita Satheesh and Dr. Ravindra Patel [International Journal on Computer Science and Engineering – Vol.1(3), 2009, Page.206-216]

for a judge to conceive of all the possible uses of information or its consequences[37] "*The creation of new knowledge complicates data privacy law as it involves information the individual did not possess and could not disclose, knowingly or otherwise. In addition, as our state becomes an "information state" through increasing reliance on information – such that information is described as the "lifeblood that sustains political, social, and business decisions. It becomes impossible to conceptualize all of the possible uses of information and resulting harms. Such a situation poses a challenge for courts who are effectively asked to anticipate and remedy invisible, evolving harms.*"[38]

The contemporary age has been aptly regarded as "an era of ubiquitous data surveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology." [39] These data sets are capable of being searched; they have linkages with other data sets; and are marked by their exhaustive scope and the permanency of collection.[40]

Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State. One of the chief concerns which the formulation of a data protection regime has to take into account is that while the web is a source of lawful activity-both personal and commercial, concerns of national security intervene since the seamless structure of the web can be

[37] Ibid [para174; Page 250]
[38] Christina P. Moniodis, "Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy", Yale Journal of Law and Technology (2012), Vol. 15 (1), at page 154
[39] Yvonne McDermott, "Conceptualizing the right to data protection in an era of Big Data", Big Data and Society (2017), at page 1
[40] Ibid, at pages 1 and 4

exploited by terrorists to wreak havoc and destruction on civilised societies.[41]

Cyber-attacks can threaten financial systems. Richard A Posner, in an illuminating article, has observed "*Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defense of national security*."[42]

Posner's formulation would indicate that the State does have a legitimate interest when it monitors the web to secure the nation against cyber-attacks and the activities of terrorists.[43] While doing so, state must nevertheless put into place a robust regime that ensures the fulfilment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law. The existence of law is an essential requirement. Second, the requirement, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against arbitrary state

[41] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others (AIR 2017 SC 4161) [Informational Privacy – Part S] [para 179 Page 253]
[42] Richard A. Posner, "Privacy, Surveillance, and Law", The University of Chicago Law Review (2008), Vol.75, at Page 251
[43] Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others (AIR 2017 SC 4161) [Informational Privacy – Part S] [para 179 Page 253]

action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not re-appreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness. The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law.[44]

During the course of the hearing of these proceedings, the Union government has placed on the record an Office Memorandum dated 31 July 2017 by which it has constituted a committee chaired by Justice B N Srikrishna, former Judge of the Supreme Court of India to review inter alia data protection norms in the country and to make its recommendations. The terms of reference of the Committee are: a) To study various issues relating to data protection in India; b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill. Since the government has initiated the process of reviewing the entire area of data protection, it would be appropriate to leave the matter for expert determination so that a robust regime for the protection of data is put into place. We expect that the Union government shall follow up on its decision by taking all necessary and proper steps.[45]

The judgment lays down nine standards to be followed by every data controller/holder of third-party's Personal Identifiable Information (PII)**:**

[44] Ibid [para 180; Page 254]
[45] Ibid [para 185; Page 260]

(i) Clear and complete notice regarding information practices, to be given to the customer; **(ii)** Opt-in and opt-out options for every customer, exercisable at any time; **(iii)** The PII should be collected only to the extent required to fulfil the purposes specified in the notice; **(iv)** The PII should be used, processed, disseminated only in accordance with the purposes specified in the notice; **(v)** Customers should be able to access, modify, and/or delete their PII at any time; **(vi)** Disclosure of PII to third-parties, will be only as provided in the notice, and after consent for the same has been received from the customers; **(vii)** Implementation of reasonable security safeguards against loss, unauthorised access, destruction, use, processing, storage, modification, deanonymization, unauthorized disclosure or other risks; **(viii)** Maintaining complete openness and transparency in implementing the above requirements/practices; and **(ix)** Accountability for adherence to the above will be with the data controller.

The above-mentioned principles in the judgment have already been laid down under the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011.

The right to privacy refers to the specific right of an individual to control the collection use and disclosure of personal information. The convergence of these advanced technologies has spawned a different set of issues concerning privacy rights and data protection, as it has made personal data accessible and communicable. There is an inherent connection between right to privacy and data protection. Data

protection should primarily reconcile these conflicting interests to information.[46]

Privacy and data protection privacy require that information about individuals should not be automatically made available to other individuals and organization without prior consent of the user. Users shall be able to exercise a substantial degree of control over the data and its access by concerned application. Data protection is legal safeguard to prevent misuse of information about individual person on a medium including computers. The adoption of administrative, technical, or physical deterrents to safeguard personal data. The concepts of privacy and data protection are intertwined, an individual's data about his personal information containing name, address, telephone numbers, profession, family, such information is often available at various places like schools, colleges, banks, directories, surveys, and on various websites where such personal information has been shared. Passing-off such information to interested third parties leads to intrusion in privacy like incessant marketing calls.[47]

The advancements and innovation in the technological sector has made it difficult for information to be protected through the ambit of confidentiality only, the coverage has to be increased to include integrity and availability so as to achieve information security. The digitization of data has created convenience in terms of availability, but the data overflow had led to difficulty in management of large data, which also includes personal and sensitive information.

Today's corporates are customer centric and the success of their business depend on user's personal preference, in temptation to have

[46] Privacy and Data Protection in India by Dr. Shiv Shankar Singh [2012 Practical Lawyer February S-2 Introduction] Published by Eastern Book Company
[47] Ibid

technological adaptation, we pass on our personal and sensitive information very easily without giving much thought concerning the access that information might provide the corporates with.[48]

For example, when we access our online banking account, and feed in our email address, we without acknowledging the fact pass on sensitive information. Ideally, the information shared is for a limited purpose only but in reality, this information is processed, transmitted and exploited for purposes without the consent or authorization of information provider. In a day we receive numerous spam calls which offer various products and services and we never realise that where the tele-caller receives the contact information, these calls are results of information we unknowingly provide at various moments while accessing applications online.

INDIAN SCENERIO - INFORMATION TECHNOLOGY ACT of 2000

The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996 in order to bring uniformity in the law of different countries.[49] The General Assembly of the United Nations by Resolution No. 51/162, dated January 30th, 1997, recommended that all states should give favourable considerations to this Model Law when they enact or revise their laws.[50] The Model law provides for equal legal treatment of users of electronic communication and paper-based communication, so does the Information Technology Act of 2000 (IT Act).

---

[48] Privacy and Data Protection in Cyberspace in Indian Environment by Shrikant Ardhapurkar, Tanu Srivastava, Swati Sharma, Mr. Vijay Chaurasiya, and Mr. Abhiskeh Vaish [International Journal of Engineering Science and Technology Vol. 2(5), 2010 Page 943]

[49] UNCITRAL - Model Law on Electronic Commerce with Guide to Enactment, 1996 [United Nations Publication Sales No.E.99. V.4]

[50] United Nations General Assembly [A/RES /51/162 dated January 30th, 1997]

India is one of the largest host of outsourced data processing in the world and could face an issue with an increase in the rate of cybercrimes, mainly due absence of an appropriate legislation.

The IT Act, contains provisions regarding cyber and related IT laws in India and delineates the scope of access that a party may have concerning data stored on a computer, computer system or computer network, the provisions of the IT Act do not address the need for a stringent data protection law being in place.

The Preamble of IT Act reflects the objectives with which the Government of India enacted the IT Act. The objectives of the Act are: (a) To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "***electronic commerce***", which involve the use of alternatives to paper-based methods of communication and storage of information; (b) To facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."[51]

The Information Technology Act of 2000 (IT Act) covers the concept of data protection and is the only Act which speaks about the issues of data protection. According to Section 2 (1) (o) of the IT Act defines Data as "*a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network and*

[51] Preamble of the Information Technology Act of 2000 (No. 21 of 2000)

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."[52]

There is no shield that cannot be pierced, no fort that cannot be breached, and no computer system that cannot be hacked. [53] IT Act tries to secure with issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data.

The IT Act provides preventive measures to be undertaken (provided in Chapters V to VIII of the IT Act). The IT Act not only provides for preventive measures to be undertaken (but also civil and criminal liability for illegal activity).

The government has notified the Information Technology *(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("Rules") were promulgated. Though the Rules attempted to elaborate further on the requirements of Section 43-A of the IT Act.[54]

---

[52] Section 2 (1) (o) of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922

[53] In this regard one may like to read the conversation between Achilles and the Tortoise under the heading Contracrostipunctus on Page 75 of the book 'Godel Escher, Bach: An Eternal Golden Briad by Douglas R. Hofstadter and chapter titles; Consistency, Completeness and Geometry'.

[54] Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000
[PRESS NOTE – Release ID: 74990]

The Rules only deals with protection of 'sensitive personal data or information of a person' which includes such personal information which consists of information relating to (a) passwords; (b) financial information such as bank account, or credit card or debit card or other payment instrument details; (c) physical, physiological and mental health condition; (d) sexual orientation; (e) medical records and history; and (f) biometric information; (g) any detail relating to the above clause as provided to body corporate for providing service; and (h) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract of otherwise, provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.[55]

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with 'personal sensitive data or information'.

Under Section 43A of IT Act inserted through an amendment in the IT Act in the year 2008, states a body corporate who is possessing, dealing or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. Section 43A of the IT Act primarily concentrates on the compensation for negligence in implementing and maintaining

[55] Section 3 of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, dated April 11th, 2011

'reasonable security practices and procedures' in relation to 'sensitive personal data of information' (SPDI).

The advent of Section 43A of the IT Act, and the rules have compelled business houses to review their contractual arrangements in order to ensure that their data security practices and procedures are at par with those that are stipulated under the law.[56] The section places an explicit importance on data protection and security, by imposing a fine of upto INR 5,00,00,000 (Rupees Five Crores Only) on any entity handles or stores sensitive personal information, but fails to implement reasonable security practices to protect that information.

Section 43A of the IT Act mandates following of 'reasonable security practices and procedures' in relation to SPDI. The International Standard IS/ISO/IEC 27001 relating to 'information-technology-security-techniques-information security management system-requirements' is one of the standards ('stipulated standard') specified under the rules that may be implemented by a body corporate while handling SPDI. If any industry association or entity is following any standard apart from the stipulated standard for data protection, they are required to get their codes approved and notified by the Government of India. Such body corporates which have implemented the stipulated standard or code need to get the same certified or audited by an independent auditor approved by the Central Government. Further, an audit has to carried out by such an auditor at least once a year or as and when there is a significant upgradation of processes and computer resources.[57]

[56] Overview of Data Privacy Laws in India and Aspects of Data Protection that account when establishing a business in India by Supratim Chakraborty and Aritri Roy Chowdhury [Khaitan & Co. LLP] Published by Association of Corporate Counsel

[57] Ibid [Reasonable Security Practices and Procedures]

Under the rules, a body corporate is required to obtain prior consent from the information provider regarding the purpose of usage of the SPDI. Such information should be collected only if it is essential and required for a lawful purpose connected with the functioning of the body corporate. The body corporate is also mandated to take reasonable steps to ensure that the information provider has knowledge about the collection of information, the purpose of collection of such information, the intended recipients and the name and address of the agency collecting and retaining the information. The information should be used only for the purpose for which it is collected and should not be retained for a period longer than what is required.[58]

The body corporate has to allow the information provider the right to review or amend the SPDI and give the information provider an option to retract consent at any point of time, in relation to the information that has been so provided. In case of withdrawal of consent, the body corporate has the option to not provide the goods or service for which the concerned information was sought.[59]

The rules specify that apart from the information sought by governmental agencies or under applicable legal provisions, a body corporate is required to obtain permission from the information provider, prior to disclosure of such information to a third party, unless such disclosure has been agreed to in an agreement between the parties.[60]

A body corporate may transfer SPDI to other body corporates, located anywhere across the globe provided that the transferee ensures the same or equal level of data protection that is adhered to by the body

[58] Ibid [Collection of Sensitive Personal Data of Information]
[59] Ibid [Collection of Sensitive Personal Data of Information]
[60] Ibid [Disclosure to Third Party]

corporate as per the Rules. However, the transfer may be permitted only if the same is necessary for the performance of lawful contract between the body corporate and information provider or where such information provider has consented to such a transfer.[61]

The Rules mandate that a body corporate handling SPDI shall provide a comprehensive privacy policy containing details such as the type of information collected, the purpose of collection of information, the disclosure policy, the security practices and procedures followed. The privacy policy is required to be clearly published on the website of the body corporate and made readily available to the information providers.[62]

Under Section 72A of the IT Act, states any person secured access to any electronic record, book, registrar, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs, 5,00,000. (US $ 8,000 Approx.)[63]

[61] Ibid [Transfer of Sensitive Personal Data of Information]
[62] Ibid [Privacy Policy]
[63] Section 72 of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922

IT Act – CIVIL LIABILITY

The Information Technology (Amendment) Act 2008 provides for civil liability in case of computer database theft, computer trespass, unauthorized digital copying, downloading and extraction of data, privacy violation.[64]

Furthermore, Section 43 provides for penalty for a wide range of cyber contraventions such as: (a) related to unauthorised access to computer, computer system, computer network or resources; (b) unauthorised digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in any media; (c) introduced any computer contaminant or computer virus into any computer system or computer network; (d) unauthorised transmission of data or programme residing within a computer, computer system or computer network; (e) computer data/database disruption, spamming etc.; (f) denial of service attacks, data theft, fraud, forgery etc.; (g) unauthorised access to computer data/computer databases; (h) instances of data theft (passwords, login IDs); (i) destroys, deletes or alters any information residing in a computer resource etc and (j) steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage. Explanation (ii) of Section 43 provisions definition of computer database as "a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and

[64] Privacy and Data Protection in India: A Critical Assessment by Shiv Shankar Singh [Journal of Indian Law Institute Volume.53:4 Page No. 663-677]

are intended for use in a computer, computer system or computer network."[65]

IT Act – CRIMINAL LIABILITY

The Information Technology (Amendment) Act, 2008 provides for criminal liability in case of computer database theft, privacy violation etc. The Act also make wide ranging amendments in Chapter XI - Sections 65-74 which cover a wide range of cyber offences, including offences related to unauthorised tempering with computer source documents,[66] dishonestly or fraudulently doing any act referred to in section 43,[67] sending offensive messages through communication service,[68] dishonestly receiving stolen computer resource or communication device,[69] identity theft,[70] cheating by personation by using computer resource,[71] violation of privacy,[72] cyber terrorism[73], transmitting obscene material in electronic form[74], transmitting of material containing sexually explicit act, in electronic form[75], transmitting of material depicting children in sexually explicit act, in electronic form[76], any intermediary intentionally or knowingly contravening the provisions of sub-section (1) of section 43[77], any person intentionally or knowingly failing to comply with any order of

[65] Section 43 of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922
[66] Ibid Section 65
[67] Ibid Section 66
[68] Ibid Section 66A
[69] Ibid Section 66B
[70] Ibid Section 66C
[71] Ibid Section 66D
[72] Ibid Section 66E
[73] Ibid Section 66F
[74] Ibid Section 67
[75] Ibid Section 67A
[76] Ibid Section 67B
[77] Ibid Section 67C

controller,[78] interception or monitoring or decryption of any information through any computer resource[79], blocking for public access of any information through any computer resource[80], intermediary contravening the provisions of sub section (2) of section 69B by refusing to provide technical assistance to the agency authorised by the Central Government to monitor and collect traffic data or information through any computer for cyber security[81], securing access or attempting to secure access to any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure[82], any misrepresentation to or suppressing any material fact from the Controller or the Certifying Authority[83], breach of confidentiality and privacy[84], disclosure of information in breach of lawful contract[85], publishing electronic signature certificate false in certain particulars[86], and electronic signature certificate for any fraudulent or unlawful purpose.[87]

[78] Ibid Section 68
[79] Ibid Section 69
[80] Ibid Section 69A
[81] Ibid Section 69B
[82] Ibid Section 70
[83] Ibid Section 71
[84] Ibid Section 72
[85] Ibid Section 72A
[86] Ibid Section 73
[87] Ibid Section 74

DIGITAL INDIA

Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy.[88]

The journey of e-Governance initiatives in India took a broader dimension in mid 90s for wider sectoral applications with emphasis on citizen-centric services. These e-Governance projects were citizen-centric, they could make lesser than the desired impact. Government of India launched National e-Governance Plan (NeGP) in 2006. In order to transform the entire ecosystem of public services through the use of information technology, the Government of India has launched the Digital India programme with the vision to transform India into a digitally empowered society and knowledge economy.[89]

The key initiatives under the Digital India scheme to push the use of technology to connect and empower people in areas relating to health, education, labour and employment, commerce. The initiatives include i.e. **(i)** Digi Locker is a service launched to target at the idea of paperless governance, DigiLocker is a platform for issuance and verification of documents & certificates in a digital way, thus eliminating the use of physical documents. Indian citizens who sign up for a DigiLocker account get a dedicated cloud storage space that is linked to their Aadhaar - Unique Identification Authority of India (UDAI) number[90] **(ii)** MyGov.in is a portal citizen-centric platform empowers people to connect with the Government & contribute towards good governance through a 'Discuss', 'Do', 'Disseminate'

[88] Digital India – Power to Empower [Ministry of Electronics & Formation Technology Government of India] http://digitalindia.gov.in/content/about-programme
[89] Ibid
[90] Unique Identification Authority of India [Government of India] https://uidai.gov.in/

approach[91]; **(iii)** eSign framework is an online electronic signature service which can be integrated with service delivery applications via an API to facilitate an eSign user to digitally sign a document[92]; **(iv)** Swach Bharat Abhiyan is an initiative "We must not tolerate the indignity of homes without toilets and public spaces littered with garbage. For ensuring hygiene, waste management and sanitation across the nation, a 'Swachh Bharat Mission' will be launched[93]; **(v)** National Scholarship portal is a one-stop solution through which various services starting from student application, application receipt, processing, sanction and disbursal of various scholarships to Students are enabled. National Scholarships Portal is taken as Mission Mode Project under National e-Governance Plan (NeGP)[94]; **(vi)** E-Hospital, is a one-stop solution for addressing these concerns and connecting patients, hospitals and doctors on the digital platform. It's a Hospital Management Information System for managing key functional areas and processes of hospitals.[95]; **(vii)** Digitize India platform, is an initiative which offers an opportunity for government agencies to transform themselves into digital enterprises[96]; **(viii)** Bharat net, National Optical Fibre Network (NOFN) is an ambitious initiative to trigger a broadband revolution in rural areas. NOFN was envisaged as an information super-highway through the creation of a robust middle-mile infrastructure for reaching broadband connectivity to Gram Panchayats. (world's largest rural broadband project using optical fibre)[97]; **(ix)** Public Wi-fi hotspots, the initiative of developing high-speed BSNL hotspots throughout the country to improve digital

[91] MyGov: An Overview https://www.mygov.in/overview/
[92] eSign [Ministry of Electronics & Information Technology] http://cca.gov.in/cca/?q=eSign.html
[93] Swachh Bharat Mission [Ministry of Housing and Urban Affairs] http://www.swachhbharaturban.in/sbm/home/#/SBM
[94] National Scholarship Portal [Ministry of Electronics & Information Technology – Government of India] https://scholarships.gov.in/aboutusPage
[95] E-Hospital (National Informatics Centre) https://www.nic.in/projects/e-hospital/
[96] Digitize India Platform https://digitizeindia.gov.in/
[97] Bharat Net (NOFN) http://vikaspedia.in/e-governance/digital-india/national-optical-fibre-network-nofn

connectivity in the country[98]; **(x)** Electronics Development Fund, it is envisaged to develop the Electronics System Design and Manufacturing (ESDM) sector to achieve "Net Zero Imports" by 2020. Setting up of Electronic Development Fund (EDF) is one of the important strategies which would enable creating a vibrant ecosystem of innovation, research and development (R&D) and with active industry involvement. The EDF will also help attract venture funds, angel funds and seed funds towards R&D and innovation in the specified areas. [99]

The government under its flagship scheme of 'Digital India' as mentioned above aims to transform the country into a digitally empowered society and make delivery of public services using online platform(s) resulting in increased access to the internet. Consequently, increasing the digital footprint which in result will increase the amount of data being generated – voluntarily or involuntarily by users.

However, the framework or a Code under which this information/data is collected, processed and stored is non-existent in India. Most of the Indians using internet have little idea about data privacy and ignore the underlying consent agreements they instinctively authorize access to, which makes them susceptible to illegal data harvesting, ID theft.

The data generated by our online electronic tracks can be analysed in ways we not even aware about. A case in point is the recent controversy around the Cambridge Analytica, which resulted due to the mass harvesting of personal data by Facebook users without their knowledge or prior consent.

[98] Public Wi-Fi Hotspots (Ministry of Electronics & Information Technology – Government of India) http://digitalindia.gov.in/content/public-wi-fi-hotspots-0
[99] Electronics Development Fund [Ministry of Electronics and Information Technology] Available at: http://meity.gov.in/esdm/edf

AADHAR (UIDAI) ISSUE – DATA PROTECTION

The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 (Aadhaar Act) enables the Government to collect identity information from citizens[100] including their biometrics, issue a unique identification number or an Aadhaar Number on the
basis of such biometric information [101] and thereafter provide targeted delivery of subsidies, benefits and services to them. [102]

Aadhaar Act establishes an authority, namely, the UIDAI, which is responsible for the administration of the said Act. It also establishes a Central Identities Data Repository (CIDR)[103] which is a database holding Aadhaar Numbers and corresponding demographic and biometric information.[104] Under the Aadhaar Act, collection, storage and use of personal data is a precondition for the receipt of a subsidy, benefit or service.[105]

Data protection norms for personal information collected under the Aadhaar Act are also found in the Aadhaar (Data Security) Regulations, 2016 (Aadhaar Security Regulations). The Aadhaar Security Regulations impose an obligation on the UIDAI to have a security policy which sets out the technical and organisational measures which will be adopted by it to keep information secure.[106]

Despite its attempt to incorporate various data protection principles, Aadhaar has come under considerable public criticism. First, though

[100] Section 30, Aadhaar Act.
[101] Section 3, Aadhaar Act.
[102] Section 7, Aadhaar Act.
[103] Section 10, Aadhaar Act
[104] Section 2(h), Aadhaar Act.
[105] Section 7, Aadhaar Act.
[106] Regulation 3, Aadhaar Security Regulations

seemingly voluntary, possession of Aadhaar has become mandatory in practice, and has been viewed by many as coercive collection of personal data by the State.[107] Concerns have also been raised vis-a-vis the provision on Aadhaar based authentication which permits collection information about an individual every time an authentication request is made to the UIDAI.[108] Finally, despite an obligation to adopt adequate security safeguards, no database is 100% secure.[109] In light of this, the contest debate on the issue of the interplay between any proposed data protection framework and the existing Aadhaar framework is one to keep a watch on.

[107] Reetika Khera, 'The Different Ways in Which Aadhaar Infringes on Privacy', The Wire (19 July 2017),
available at https://thewire.in/159092/privacy-aadhaar-supreme-court/
[108] Jean Dreze, 'Hello Aadhaar, Goodbye Privacy', The Wire (24 March, 2017) available at
https://thewire.in/118655/hello-aadhaar-goodbye-privacy/
[109] Subhashis Banerjee *et al.*, A Computer Science Perspective: Privacy and Security of Aadhaar, 52(37) Economic & Political Weekly (16 September 2017).

5. LAST MILE – DATA PROTECTION IN INDIA

India's digital economy is characterized by 'last mile' data protection with privacy norms and data collection/sharing standards being set at the level of the application operating system ('OS') and the device. This practice leads to multiple, often overlapping/criss-cross policies maintained by smartphone manufacturers, mobile operating system vendors and application developers. The important question that needs to be asked is (a) what data is collected; (b) where it is stored; (c) who it is shared with; and (d) legal recourse in the face of policy violations or unauthorized use of data by third parties.[110]

The digital ecosystem in India is marked with a reliance on imported products and services, and along with them an imported standard of data protection. The policies and terms of engagement between a series of actors i.e. mobile operating system, device manufacturer, the application and the user, create a complex and incongruous set of standards for India's digital economy. These 'last mile' policies erode the capacity of the Indian state to protect the data of its citizen, even as it has belatedly begun the pursuit of this goal through judicial pronouncement.

INCONGRUOUS MESH OF PRIVACY STANDARDS – POLICIES OF MAJOR TECHNOLOGY OPERATORS IN INDIA

1. GOOGLE PLAY DEVELOPER DISTRIBUTION AGREEMENT

All developers who seek to make their applications available through Google Play (App store) for the company's Android operating system are

[110] Working with Last Mile Data Protection in India by Arun Sukumar [Asie. Visions. No. 96, Ifri – Centre for Asian Studies, November, 2017] page.no.5-21

required to sign a Developer Distribution Agreement (DDA) with the app store. The DDA stipulates that developers are required to provide 'legally adequate privacy notice and protection.[111] The agreement makes it abundantly clear that 'if the user has opted into a separate agreement with (the developer) to store or use personal or sensitive information directly related to the (the application) then the terms of that agreement will govern your use of such information.'[112]

GOOGLE DEVELOPER POLICY – ANDROID CORE APPLICATION STANDARDS

The Google developer policy also contains similar data protection norms, where the application is required, according to the policy, to comprehensively disclose how (the) application collects, uses and shares user data, including the types of parties with whom it's shared.[113]

Android application developers are expected to meet a series of requirements to satisfy security and functionality condition. For instance: (a) All private data should be stored in the application's internal storage; (b) All external data should be verified before being accessed; and (c) Applications should only request the absolute minimum permissions required to support core functionality.[114] The application does not seek permission to access 'sensitive data' unless required for a core capability.

[111] Clause 4.3 Google Play Developer Distribution Agreement, Available at: https://play.google.com
[112] Ibid
[113] Privacy and Security – Google Developer Policy Centre, Available at: http://play.google.com
[114] Android Developers: Core Application Quality: https://developer.android.com

Android's compatibility requirements also limit the right of developers to use the device's audio and camera functionalities. [115] Developers also have to conform to the set of the technical standards known as 'Application permissions' if they wish to make their applications available on Android. These permissions are classified as below (i) Normal; (ii) Signature; (iii) dangerous based on the type of access they seek.[116]

(i) Normal permissions allow applications access to isolated application level features, with minimal risk to other applications, the system or the user.

(ii) Signature permissions have to be requested by an application with the same digital certificate as the application that declared it.

(iii) Dangerous permissions, in contrast, offer access to private user data or control over the device that can negatively impact the user. These may require the affirmative consent before the user.

The protection level required for an application to access fingerprint hardware in Android phones for example is normal.[117] On the other hand, the ability by an application to send SMSs, access user location, answer phone calls, and track body metrics require dangerous permissions.[118] Finally developers, also have to ensure that some properties of their applications are out of bounds for third party applications, such as rebooting an OS, or capturing audio and video.[119]

These agreement/policies incubate the guidelines and standards that ought to be maintained by application developers on Android platforms.[120]

[115] Ibid
[116] Application Manifest: Android Developers – https://developer.android.com
[117] Normal Permissions: Android Developers – https://developer.android.com
[118] Requesting Permissions: Android Developers – https://developer.android.com
[119] Manifest Permission: Android Developers – https://developer.android.com
[120] Working with Last Mile Data Protection in India by Arun Sukumar [Asie. Visions. No. 96, Ifri – Centre for Asian Studies, November, 2017] page.no.5-21

India does not have specific data protection legislation, other than the IT
Act, which provides the authorities discretionary authority to monitor and collect traffic data, and possibly other data. The IT Act does not impose data quality obligations in relation to personal information and does not impose obligations on private sector organizations to disclose details of the practices in handling personal and sensitive information.

India is experiencing a number of litigations which are throwing up questions on data privacy and data protection that were never addressed before. Recently, the Supreme Court of India in the case of Karmanya Singh Sareen & Another v. Union of India & Others (UOI)[121] concerns raised in a writ petition on WhatsApp's data sharing policy, after its acquisition by Facebook Inc. The issues sought to be raised relates to the protection of privacy of details and data of users (including chats, photos, videos, voice messages, files, and share location information) of WhatsApp. When "WhatsApp" was launched in the year 2010, it had declared a privacy policy of total/complete safety against any kind of sharing of data/details of users and in view of the complete security and protection of privacy provided by WhatsApp. Though a change has been proposed to be made in the privacy policy of WhatsApp after its acquisition, that the account information would be shared with Facebook and all its group companies for the purpose of commercial advertising and marketing amounting to infringement of right of privacy of the user as claimed by the petitioner.

The Court held the fact that under the Privacy Policy of "WhatsApp", the users are given an option to delete their "WhatsApp" account at any time, in which event, the information of the users would be deleted from the servers of "WhatsApp". Therefore, the court is of the view that it is always open to the existing users of "WhatsApp" who do not want

[121] Karmanya Singh Sareen & Another v. Union of India & Others 2016 (68) PTC 486 (Del)

their information to be shared with "Facebook", to opt for deletion of their account. Further, if the users opt for completely deleting "WhatsApp" account before September, 2016, the information/data/details of such users should be deleted completely from "WhatsApp" servers and the same shall not be shared with the "Facebook" or any one of its group companies; (ii) So far as the users who opt to remain in "WhatsApp" are concerned, the existing information/data/details of such users upto 25.09.2016 shall not be shared with "Facebook" or any one of its group companies; and (iii) Respondents shall consider the issues regarding the functioning of the Internet Messaging Applications like “WhatsApp” and take an appropriate decision at the earliest as to whether it is feasible to bring the same under the statutory regulatory framework.

6. DATA PROTECTION FRAMEWORK FOR INDIA[122]

Government of India cognizant of the growing importance of data protection in India, and the need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance. It has thus decided to constitute a Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, former judge of Supreme Court of India, to identify key data protection issues in India and recommend methods of addressing them.[123]

The 21st century has witnessed such an explosive rise in the number of ways in which we use information, that it is widely referred to as 'the information age'. It is believed that by 2020, the global volume of digital data we create is expected to reach 44 zettabytes.[124]

With the rapid development of technology, computers are able to process vast quantities of information in order to identify correlations and discover patterns in all fields of human activity. Enterprises around the world have realised the value of these databases and the technology for its proper mining and use is evolving every day.

---

[122] White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017

[123] Office Memorandum No.3 (6)/2017 – CLES (Ministry of Electronics & Information Technology – Government of India) – Constitution of a Committee of Experts to deliberate on a data protection framework for India

[124] The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC (April 2014), available at:https://www.emc.com/leadership/digital universe/2014iview/executive-summary.html

Proprietary algorithms are being developed to comb this data for trends, patterns and hidden nuances by businesses.[125]

While the transition to a digital economy is underway, the processing of personal data has already become ubiquitous in both the public and private sector. Data is valuable per se and more so, when it is shared, leading to creation of considerable efficiency. The reality of the digital environment today, is that almost every single activity undertaken by an individual involves some sort of data transaction or the other. The Internet has given birth to entirely new markets: those dealing in the collection, organisation, and processing of personal information, whether directly, or as a critical component of their business model.[126] As has been noted by the Supreme Court in Puttaswamy.[127]

'Uber', the world's largest taxi company, owns no vehicles. 'Facebook', the world's most popular media owner, creates no content. 'Alibaba', the most valuable retailer, has no inventory. And 'Airbnb', the world's largest accommodation provider, owns no real estate.'[128]

In today's world, even to hail a taxi involves use of an application which involves feeding user related information/data on the application, most importantly real-time location services, user's financial information, and information concerning previous trips, all

---

[125] Big data: Changing the Way Businesses Operate and Compete', Ernst & Young (April 2014)
[126] Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review 357 (2005).
[127] Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. [2017 (10) SCALE 1]
[128] Tom Goodwin, 'The Battle is for Customer Interface', TechCrunch (3 March 2015), available at: https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/Cited in Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors. [2017 (10) SCALE 1], Per S.K. Kaul, J. at paragraph 17.

this digitized data is stored, and processed by these travel applications for internal/external purposes and stored in their servers.

Data is fundamentally transforming the way individuals do business, how they communicate, and how they make their decisions. Business are now building vast databases of consumer preferences and behaviour. Information can be compressed, assorted, manipulated, discovered and interpreted as never before, and can thus be more easily transformed into useful knowledge.[129] The low costs of storing and processing information and the ease of data collection has resulted in the prevalence of long-term storage of information as well as collection of increasingly minute details about an individual which allows an extensive user profile to be created.[130] Then such information is used to create customised user profiles by analytical firms, based on their past online behaviour, which has the benefit of reducing the time required to complete a transaction. For instance, e-commerce websites track previous purchases, use algorithms to predict what sorts of items a user is likely to buy, thereby reducing the time spent on each purchase. [131]

Recommendation algorithms are best known for their use on e-commerce Web sites[132], where they use input about a customer's interests to generate a list of recommended items. Recommendation algorithms start by finding a set of customers whose purchased and

---

[129] Helen Nissenbaum, 'Privacy in Context-Technology, Policy, and the Integrity of Social Life', 36, (Stanford University Press, 2010).
[130] Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', 52 Stanford Law Review 1315 (1999).
[131] For an illustrative example, see Industry Report – Amazon.com Recommendations (Item to Item Collaborative Filtering) by Gren Linden, Brent Smith, and Jeremy York – Published by the IEEE Computer Society – January – February, 2003
https://www.cs.umd.edu/~samir/498/Amazon-Recommendations.pdf
[132] J.B. Schafer, J.A. Konstan, and J. Reidl, "E-Commerce Recommendation Applications," Data Mining and Knowledge Discovery, Kluwer Academic, 2001, pp. 115-153.

rated items overlap the user's purchased and rated items.[133] The algorithm aggregates items from these similar customers, eliminates items the user has already purchased or rated, and recommends the remaining items to the user. Two popular versions of these algorithms are collaborative filtering and cluster models. Other algorithms — including search-based methods and our own item-to-item collaborative filtering — focus on finding similar items, not similar customers. For each of the user's purchased and rated items, the algorithm attempts to find similar items. It then aggregates the similar items and recommends them.[134]

In India, the state uses personal data for purposes such as the targeted delivery of social welfare benefits, effective planning and implementation of government schemes, counter-terrorism operations. Such collection and use of data is usually backed by law, though in the context of counter-terrorism and intelligence gathering, it appears not to be the case.[135]

These technological developments have been the biggest obstacle in regulating emerging technologies such as Big Data, artificial

---

[133] P. Resnick et al., "GroupLens: An Open Architecture for Collaborative Filtering of Netnews," Proc. ACM 1994 Conf. Computer Supported Cooperative Work, ACM Press, 1994, pp. 175-186.

[134] Industry Report – Amazon.com Recommendations (Item to Item Collaborative Filtering) by Gren Linden, Brent Smith, and Jeremy York – Published by the IEEE Computer Society – January – February, 2003 [Recommendation Alogrithms]

[135] Press Information Bureau, 'Home minister proposes radical restructuring of security architecture', Ministry of Home Affairs, Government of India (23 December 2009), available at http://pib.nic.in/newsite/erelease.aspx?relid=56395;
Press Information Bureau, 'Centralised System to Monitor Communications', Ministry of Communications, Government of India (26 November 2009), available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=54679;
Udbhav Tiwari, 'The Design and Technology behind India's Surveillance Programme',
Centre for Internet & Society, India (20 January 2017), available at https://cis-india.org/internetgovernance/blog/the-design-technology-behind-india2019s-surveillance-programmes

intelligence and the Internet of Things, lies in the fact that they operate outside the framework of traditional privacy principles. These principles, as they were originally envisaged, were designed to protect a single static data set. [136] The advent of such technologies has also expanded the very definition of personal data. For instance, analysing meta-data such as a set of predictive or aggregated findings, or by combining previously discrete sets of data, Big Data has radically expanded the range of personally identifiable data.[137] Data which is viewed as non-personal information can now be combined with other data sets to create personally identifiable information. An example of this is how anonymised Netflix data on ranking of films could be easily combined with other data sets such as timestamps with public information from the Internet Movie Database (IMDb) to de-anonymise the original data set and reveal personal movie choices.[138] Similarly, Big Data relies on accumulation of large volumes of data to extract knowledge from them, making it difficult to apply the principle of data minimisation.[139]

Additionally, technologies such as the Internet of Things (IoT) relies on continuous collection of personal information from the users of 'smart devices', which may then be interpreted to provide unique services.[140]

---

[136] Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and Models', 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x

[137] Kate Crawford and Jason Schultz, 'Big Data And Due Process: Towards A Framework To Redress Predictive Privacy Harms', 55(1) Boston College Law Review 93 (2014).

[138] Bruce Schneier, 'Why 'anonymous' data sometimes isn't', Wired (12 December 2017), available at: https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/

[139] Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and Models', 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x

[140] Article 29 Data Protection Working Party Opinion, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', European Commission (16 September 2014), available at: http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Therefore, in such instances as well, it may be difficult to adhere to the traditional privacy principles of consent, collection and use limitation. Given the dynamic pace of development of emerging technologies, alternatives to traditional privacy principles have thus been suggested that require careful scrutiny.[141]

CONSENT – TO SHARE DATA

Consent forms the foundation of data protection, and use that consent as a validating mechanism for data processing and also satisfying two needs. Firstly, consent is intuitively considered as the most appropriate method to ensure the protection of an individual's autonomy.[142] Allowing an individual to have autonomy over her personal information allows her to enjoy "informational privacy". Informational privacy may be broadly understood as the individual's ability to exercise control over the manner in which her information may be collected and used.[143] Second, consent provides a "morally transformative" value as it justifies conduct, which might otherwise be considered wrongful.[144] For instance, seeking consent is what differentiates from taking possession of another individual's object, from theft.

It is estimated that globally, one in three Internet users is a child under the age of 18.[145] Although Internet-use among children is very

[141] Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and
Models', 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x

[142] In democratic societies, there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth and in the need to maintain social processes that safeguard his sacred individuality." *See:* Alan Westin, 'Privacy and Freedom', (Atheneum, 1967).

[143] Adam Moore, 'Toward Informational Privacy Rights', 44 San Diego Law Review 809 (2007).

[144] John Kleinig, 'The Nature of Consent' in 'The Ethics of Consent - Theory and Practice', 4 (Alan Wertheimer
and Franklin Miller (*eds.*), Oxford University Press, 2009).

[145] Sonia Livingstone *et al.*, 'One in Three: Internet Governance and Children's Rights', Global Commission on Internet Governance Paper Series No. 22

common and children are becoming more familiar with technology, they are viewed as being more vulnerable than adults online. They may be more easily misled, given their lack of awareness with respect to the long-term consequences of their actions online.[146] Therefore, children represent a vulnerable group, which may benefit from receiving a heightened level of protection with respect to their personal information.[147] Therefore, several jurisdictions have recognised the need to introduce data protection measures that are specifically applicable to the processing of children's personal information.

(November 2015), available at:
https://www.cigionline.org/sites/default/files/no22_2.pdf

[146] Milda Macenaite and Eleni Kosta, 'Consent for Processing Children's personal data in the EU: Following in US footsteps?', 26(2) Information & Communications Technology Law Journal (2017), available at:
http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096

[147] Children's data protection and parental consent: A best practice analysis to inform the EU data protection reform, Advertising Education Forum (October 2013), available at:
http://www.aeforum.org/gallery/5248813.pdf

7. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT ("OECD")

The OECD[148] (Organisation for Economic Co-operation and Development) has formulated Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("the Guidelines"), which state that 'the development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data'.[149]

OECD Guidelines have inspired multiple data protection frameworks such as the European Directive 95/46/EC on the processing of personal data and the free movement of such data (Data Protection Directive), the 2004 Asia-Pacific Economic Cooperation Framework (APEC Framework) as well as data protection legislations such as the

[148] http://www.oecd.org OECD is an organization that provides governments a setting in which to discuss, develop and perfect economic and social policy. They compare experiences, seek answers to common problems and work to co-ordinate domestic and international policies that increasingly in today's globalised world must form a web of even practice across nations.
[149] For the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data refer to: http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

Australia's Privacy Act, 1988 (Privacy Act), New Zealand's Privacy Act, 1993 and Japan's Protection of Personal Information Act, 2003.[150]

The Guidelines create a balance between the protection of privacy and individual liberties and the advancement of free flows of personal data through eight privacy principles i.e. **(i)** Collection Limitation principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject; **(ii)** Data Quality principle - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date; **(iii)** Purpose Specification principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose; **(iv)** Use Limitation principle - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with except: a) with the consent of the data subject; or b) by the authority of law. **(v)** Security safeguards principle - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data; **(vi)** Openness principle - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and

[150] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

the main purposes of their use, as well as the identity and usual residence of the data controller; **(vii)** Individual Participation principle - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended; and **(viii)** Accountability principle - A data controller should be accountable for complying with measures which give effect to the principles stated above. When, if observed, are supposed to guarantee a free flow of personal information from other OECD countries[151].

OECD Guidelines as updated in 2013 (2013 OECD Guidelines) keep the core privacy principles such as collection limitation, data quality and purpose specification etc. intact, several new elements to strengthen data safeguards have been introduced. These include: privacy management programs to enhance accountability of the data controller,[152] data security breach notification[153] which oblige data controllers to inform individuals/authorities of a security breach and establishment and maintenance of privacy enforcement authorities[154].

---

[151] OECD Privacy Principles - A data controller should be accountable for complying with measures which give effect to the principles stated above.
[152] Privacy management programmes are intended be integrated in the governance structure of a data controller and establish appropriate internal oversight mechanisms to ensure data is safeguarded (Organisation for Economic Co-operation and Development, 'Thirty Years After: The OECD Privacy Guidelines' (2011),
available at: http://www.oecd.org/sti/ieconomy/49710223.pdf
[153] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf
[154] Ibid

Further cross-border flows of data[155] and international cooperation to improve global interoperability of privacy frameworks have been recognised as essential for a global data economy.[156]

India is not a member of the OECD, but in the year 2001 it became the 27th member of the Development Centre, a semi-independent body within the OECD that works to foster policy dialogue and understanding between OECD countries and the developing world.

2013 OECD Guidelines have been criticised as being fundamentally incompatible with modern technologies and Big Data analytics which have revolutionised how data is collected and processed.[157]

[155] Ibid
[156] Ibid
[157] Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and Models', 1(1) Data Science and Engineering (March 2016), available at: https://link.springer.com/article/10.1007/s41019-015-0001-x

8. COMPARATIVE APPROACHES - DATA PROTECTION

In determining, India's approach to data protection, it will be instructive and illustrative to have a comparative analysis of data protection practices in other jurisdictions.

EUROPEAN UNION (EU) – General Data Protection Regulation

Data/information helps corporates distinguish themselves and create a competitive edge in the market, but concerns have been growing over the way corporates have been use this consumer data for marketing. EU, has legislation a regulation which has taken lead in amending its existing data protection laws through introduction of General Data Protection Regulation (GDPR), with more stringent compliance, in cases failure to comply the fines is up to 4% of company's annual global revenue.

The European Union has taken the lead in amending its existing data protection laws through the introduction of GDPR. In EU, the right to privacy is a fundamental right which seeks to protect an individual's dignity.[158]

The European Charter of Fundamental Rights (EU Charter) recognises the right to privacy as well as the right to protection of

[158] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).

personal data, in Article 7[159] and Article 8[160]. The first principal EU legal instrument on data protection was the Data Protection Directive.[161] The Data Protection Directive was significantly inspired by the OECD guidelines,[162] and sought to achieve a uniformly high level of data protection in the EU by harmonising data protection legislations in order to ensure that free flow of data was not impeded.[163] The Data Protective Directive was eventually adopted as national legislations by EU member States. Given that it was a non-binding instrument, it left some room for interpretation.[164]

The rapidly changing data landscape led the EU to update its regulatory environment on data protection.[165] The product of this process is the EU General Data Protection Regulation of 2016 (EU GDPR). The EU GDPR is considered to be one of the most stringent

[159] Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications.
[160] Protection of personal data -(1) Everyone has the right to the protection of personal data concerning him or her; (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; and (3) Compliance with these rules shall be subject to control by an independent authority.
[161] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, 'Handbook on European Data Protection Law' (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
[162] OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[163] The European Union Agency for Fundamental Rights (FRA), the Council of Europe and the Registry of the European Court of Human Rights, 'Handbook on European Data Protection Law' (2014), available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
[164] The EU GDPR, 'How did we get here?', available at http://www.eugdpr.org/how-did-we-get-here-.html
[165] Ibid

data protection laws in the world[166] and being a regulation, it will become immediately enforceable as law in all Member States. However, given the ambitious changes it envisages, Member States have been given two years (till 25 May 2018) to align their laws to the EU GDPR.

The EU GDPR is a comprehensive data protection framework which applies to processing of personal data by any means, and to processing activities carried out by both the Government as well as the private entities, although there are certain exemptions such as national security, defence, public security.[167] The EU GDPR follows a rights-based approach towards data protection and places the individual at the centre of the law. As a consequence, it imposes extensive control over the processing of personal data both at the time of, and after the data has been collected.[168]

Further, collection of certain forms of personal data, known as sensitive personal data (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health and sex life) is prohibited subject to certain exceptions.[169] Thus, for processing to be lawful and fair, the entity collecting personal data must comply with an extensive range of principles such as that of purpose specification,[170] data minimisation,[171] data quality,[172] security safeguards.[173]

---

[166] DLA Piper, 'EU General Data Protection Regulation' available at https://www.dlapiper.com/en/asiapacific/focus/eu-data-protection-regulation/home

[167] Article 23, EU GDPR.

[168] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005)

[169] Article 9, EU GDPR

[170] Article 5(1)(b), EU GDPR.

The EU model also envisages an independent supervising authority (a regulator) who is armed with an array of functions and powers.[174] Primarily, this body is responsible for monitoring and enforcing compliance with the law and for ensuring the protection of the fundamental rights in relation to processing and facilitating the free flow of data.[175]

The GDPR states that in assessing whether consent has been freely given, account shall be taken, for example, of whether the performance of a contract is made conditional on the consent to processing data that is not necessary to perform that contract. This may affect some e-commerce services, among others. In addition, Member States may provide more specific rules for use of consent in the employment context. The Recitals add that consent is not freely given if the data subject had no genuine and free choice or is unable to withdraw or refuse consent without detriment. Where personal data is processed for direct marketing the data subject will have a right to object. This right will have to be explicitly brought to their attention.[176]

A user consent to processing of their personal data must be as easy to withdraw as to give. Consent must be "explicit" for sensitive data. The data controller is required to be able to demonstrate that consent was given. Existing consents may still work, but only provided they meet the new conditions. Where personal data is processed for direct marketing the data subject will have a right to

---

171 Article 5(1)(c), EU GDPR.
172 Article 5(1)(d), EU GDPR.
173 Article 5(1)(f), EU GDPR.
174 Articles 4(21) and 51, EU GDPR.
175 Section 51, EU GDPR.
176 The EU General Data Protection Regulation, 2017 - CONSENT [ALLEN & OVERY] page.no. 4

object. This right will have to be explicitly brought to their attention.[177]

GDPR establishes a tiered approach to penalties for breach which enables the DPAs to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and EUROS 20 million (Ex. breach of requirements relating to international transfers or the basic principles for processing, such as conditions for consent). Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and EUROS 10 million.[178]

[177] Ibid
[178] Ibid – FINES – page.no. 5

UNITED STATES OF AMERICA - LEGISLATIONS

In the Unites States of America (U.S.A), privacy protection is essentially a 'liberty protection' i.e. protection of the personal space from government. [179] Thus, the American understanding of the 'right to be let alone' has come to represent a desire for as little government intrusion as possible.[180] While there is no provision in the US Constitution that explicitly grants a right to privacy, the right in a limited form is reflected in the Fourth Amendment to the US Constitution – the right against unreasonable searches and seizures. US Courts however, have collectively recognized a right to privacy by piecing together the limited privacy protections reflected in the First, Fifth, and Fourteenth amendments to the US Constitution.[181]

In addition, to the distinction in the conceptual basis of privacy, the US approach towards privacy and data protection varies from the EU in multiple respects. First, unlike the EU, there is no comprehensive set of privacy rights/principles that collectively

[179] Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).
[180] Ibid
[181] *Roe v. Wade* 410 U.S. 113 (1973) and *Griswold v. Connecticut* 381 U.S. 479 (1965). See Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review 357 (2005)

address the use, collection and disclosure of data in the US.[182] Instead, there is limited sector specific regulation.[183]

Second, the approach towards data protection varies for the public and private sector. The activities and powers of the Government vis-à-vis personal information are well defined and addressed by broad, sweeping legislations[184] such as the Privacy Act, 1974 which is based on the FIPPS (governing collection of data by the federal government); the Electronic Communications Privacy Act, 1986; the Right to Financial Privacy Act, 1978.

For the private sector, which is not governed by these legislations, certain sector-specific norms exist. These include: The Federal Trade Commission Act (FTC Act), The Financial Services Modernization Act (Gramm-Leach-Bliley Act or the GLB Act), The Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA). In addition, States have their own data protection laws.[185]

As far as private sector regulation is concerned, the core of data protection practice in the US is notice and consent. The Federal Trade Commission (FTC), is a bipartisan federal agency with the dual mission to protect consumers and promote competition[186] which has the responsibility to ensure consumer privacy enforcement. It does this by bringing enforcement actions against

[182] Joel R Reidenberg, 'Data Protection in the Private Sector in the United States' 3 International Yearbook of Law Computers and Technology (1993).
[183] Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review 357 (2005).
[184] Ibid
[185] White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017 [page.no. 13]
[186] FTC, 'What we do', available at https://www.ftc.gov/about-ftc/what-we-do

companies which violate consumer privacy, including activities like failing to comply with posted privacy principles and unauthorised disclosure of personal data. The FTC has described notice to be 'most fundamental principle'[187], and has focused all of its privacy related efforts on getting websites to post privacy policies and its enforcement efforts in holding websites accountable when they fail to adhere to them.[188]

The US approach to data protection thus has two discernible trends— stringent norms for government processing of personal information; and notice and choice-based models for private sector data processing. This dichotomy can largely be said to be a consequence of the *'laissez faire'* culture of the US markets,[189] as opposed to the rights-centric culture of the EU.[190]

[187] Martha K. Landesberg *et al.,* 'Privacy Online: A Report to Congress', FTC (June, 1998) available at: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf

[188] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).

[189] Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review 357 (2005).

[190] White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017 [page.no. 14]

9. DATA PROTECTION – ISSUES

In the past, due to limited space availability in expensive date warehouses, considerable effort was put into choosing and organizing data to ensure that only valuable data were kept for extended periods of time. Now, this view has changed. With many new technologies and tools, companies are beginning to store everything in horizontally scaled, commercial (commodity) off-the-shelf hardware. The value of the big data ecosystem is to collect make sense of this large volume of raw data and convert it into useful information.[191]

The other end of the spectrum, regulators and society as a whole are increasingly concerned about how data are being handled by business. The area of data privacy is becoming a greater concern in the post-Snowden[192] era. These giant pools of data represent tempting targets for surveillance by various security agencies, not to mention repurposing by commercial entities.[193]

[191] Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu [Ph.D, CISM, CRISC, CISSP, CSSLP] ISACA Journal Volume 3 (2014) page.no. 1 to 5

[192] Gallegos, Raul; "Edward Snowden's Sad and Lonely Future," Bloomberg Publishing, 5 November 2013, www. bloomberg.com/news/2013-11-05/edward-snowden-s-sadand-lonely-future.html

[193] Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu [Ph.D, CISM, CRISC, CISSP, CSSLP] ISACA Journal Volume 3 (2014) page.no. 1 to 5

The borderless nature of internet raises jurisdictional issues in data protection. The act of processing of personal data could occur across jurisdictions. The traditional principle of sovereignty needs to be evolved in these circumstances where such cross-border events occur. Broadly, the territory of a State is where its jurisdiction ends and States are prohibited from exercising jurisdiction in the territory of another State, unless so permitted under a treaty or customary law.[194]

The frequency of cross border actions on the Internet might require some thinking outside the framework of these principles.[195] The legislation adhering to the notion of territoriality will fail adequately to protect the individuals. Second, the ease of cross border transactions on the Internet means that foreign parties can effectively transact in India without having any office or establishment in India while ostensibly maintaining their status as entities not subject to the jurisdiction of Indian law. The nature of cloud data as a location-independent, mobile asset also poses similar jurisdictional difficulties.[196] Every act on the Internet which has a local dimension cannot be regulated by a State.

For instance, the fact that a foreign website can be accessed in India would not by itself furnish a ground for subjecting that website to Indian law. Such a law might have the undesired effect of

[194] "S.S. Lotus" (*France v. Turkey*), 1927 PCIJ (SER.a) No. 10
[195] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87 (2012); Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', University of Cambridge Faculty of Law Research Paper No. 49/2015 (30 August 2015).
[196] Andrew Keane Woods, 'Against Data Exceptionalism', 68(4) Stanford Law Review 729 (April 2016).

legislating to govern the entire Internet. [197] In the context of data protection, jurisdiction must be considered from the perspective of investigative powers, the exercise of judicial power and enforcement of laws. The last of these factors, enforceability can serve as a key objective determinant of the extent of applicability of the law.[198]

Article 3 of the GDPR – EU sets out the territorial scope of the said regulation. Clause (1) states that the regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union. Clause (2) widens the reach of the regulation by making it applicable to processing of personal data of data subjects who are in EU by controllers and processors outside the EU, if the processing activities are related to the offering of goods and services to persons in the EU or if the behaviour of such persons in the EU is monitored by such activities. While the first clause incorporates the territorial principle as in the earlier Data Protection Directive, the newer rules in clause (2) incorporate the principles of passive personality and objective territoriality with the intent of protecting the privacy of EU residents against cross border action. [199]

---

[197] *Bodil Lindqvist v. Åklagarkammaren i Jönköping*, Case C-101/01 (2003), European Court of Justice, the Court noted: 'If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an Internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the Internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the Internet.

[198] Christopher Kuner, 'Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law', University of Cambridge Faculty of Law Research Paper No. 49/2015, 16 (30 August 2015).

[199] Dan Jerker B. Svantesson, 'Extraterritoriality in the context of Data Privacy Regulation', 7(1) Masaryk University Journal of Law and Technology 87 (2012).

Personal data is a critical element which determines the zone of informational privacy guaranteed by a data protection legislation. The object of defining personal data or personal information is to demarcate facts, details, or opinions that ear a resemblance to an individual's identity. So, the information must be such that the individual is either identified or identifiable from such information.

The terms information and data are both used in the context of informational privacy and data protection. The IT Act draws a distinction between these terms. Under Section 2 (1) (v) of the IT Act "information" includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro-film or computer generated micro-fiche.[200]

Subsection (o) of the same section defines data as "data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised 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.[201] SPDI Rules under the IT Act, building on these definitions of data and information, grant protection to a category of information termed 'sensitive personal information or sensitive personal data.'[202]

[200] Section 2 (1)(v) of of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922
[201] Ibid - Section 2 (1)(o)
[202] Rule 3 - (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000 [PRESS NOTE – Release ID: 74990]

The object of data protection legislations as stated above is to ensure autonomy of the individual by protecting personal data. The individual is either identified or identifiable from such information, so the information must be such that the individual is either identified or identifiable from such information. The question of identifiability being one of context, it is essential to prescribe standards by which data can be said to be identifiable or not. the notion of identifiability are the techniques of pseudonymisation and anonymisation. Pseudonymisation refers to the technique of disguising identities which ordinarily does not exclude data from the scope of personal data. Anonymisation, by contrast, refers to data where all identifying elements have been eliminated from a set of personal data. No element may be left in the information which could, by exercising reasonable effort, serve to re-identify the person(s) concerned.[203]

Some legislations make it explicit whether information constitutes personal information is not dependent on its accuracy. A noteworthy feature of the Protection of Personal Information Act, 2013 (POPI Act) is that the definition has an illustrative component as well which lists some of the common forms of personal information.[204]

To facilitate the cross-border transfers of data, the EU has created three mechanisms under GDPR, which include 'adequacy test' set out under Article 45 of GDPR – EU[205], Model contractual clauses[206]

[203] White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017 [Chapter 3: What is Personal Data? – page.no. 34-37]
[204] Section 2, Protection of Personal Information Act, 2013
[205] Article 45, General Data Protection Regulation – EU
[206] European Commission, 'Model Contracts for the Transfer of Personal Data to Third Countries', available at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

and binding corporate rules (BCR)[207] to ensure stringent and prescriptive compliance and protect illegal harvesting of data without user consent.

(i) **Adequacy Test** - Article 45 of the EU GDPR[208] provides for an adequacy test for transfer of personal data to a third country. This test stipulates that personal data of EU subjects to non-European Economic Area or EEA countries is not permitted unless those countries are deemed to have an "adequate" level of data protection.

(ii) **Model contractual clauses** - European Commission has the power to decide that certain standard contractual clauses offer sufficient safeguards with respect to data protection while undertaking transfer of data to non-EU/EEA countries.[209] the European Commission has issued two sets of standard contractual clauses: one for transfers from data controllers to data controllers established outside the EU/EEA; and one set for the transfer to processors established outside the EU/EEA.[210]

(iii) **BCR** - BCRs define the global policy of the multi-national group of companies with regard to the international transfers of personal data within the same corporate group, to entities

[207] Ibid
[208] Article 45, General Data Protection Regulation – EU
[209] European Commission, 'Frequently Asked Questions Relating to Transfers of Personal Data From The EU/EEA To Third Countries', 11, (2009), available at: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf
[210] European Commission, 'Model Contracts for the Transfer of Personal Data to Third Countries', available at: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

located in countries, which do not provide an adequate level of protection.[211]

As, electronic commerce has become more pervasive, concerns have grown about the compatibility of various data privacy and protection regulation in the context of cross-border trade in relation under data privacy and protection regimes.[212] There have been various regulatory frameworks i.e. the EU Data Protection Directive (Directive 95/46/EC)[213] released in October 1995 to provide a basic framework for proper handling of personal information, which has been superseded by the GDPR code.

In response to the EU Data Protection Directive, countries have aligned their legislation with the Asia Pacific Economic Cooperation Privacy Framework (APEC). The APEC and OECD framework were created to ensure that States would create compatible regulation to ensure smooth interstate commerce and other forms of interaction. Both APEC and OECD have similar data protection and privacy principles. The following is a review of **8** principles in the context of the concerns regarding data protection:[214]

---

[211] European Commission, 'Overview on Binding Corporate Rules', available at: http://ec.europa.eu/justice/dataprotection/international-transfers/binding-corporate-rules/index_en.htm

[212] Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu [Ph.D, CISM, CRISC, CISSP, CSSLP] ISACA Journal Volume 3 (2014) page.no. 1 to 5

[213] The European Parliament and the Council of the European Union, EU Data Protection Directive, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995

[214] Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu [Ph.D, CISM, CRISC, CISSP, CSSLP] ISACA Journal Volume 3 (2014) page.no. 1 to 5

(a) Collection limitation—This is the first principle in both the OECD and APEC frameworks, and it is also the principle that big data can potentially violate the most. Basically, it requires that only the minimum amount of data required for a specific purpose be collected and then retained only for the minimum amount of time required. One of the key selling points of big data and the advent of cheap storage is to collect everything and throw away nothing, with the further manipulation and analysis of data occurring later. It is important that organizations moving toward big data harvesting of information and update the purposes of their applications to ensure that they remain within the spirit of this principle. An additional approach that is taken by some is to anonymize data. This process is sometimes called de-identification, where identifying ties to an individual are removed prior to the storage of large volumes of transaction data. However, care must be taken here. The simple removal of primary customer indexes might not suffice, as customer-specific information might be extrapolated from seemingly anonymous transaction data. This form of reidentification is a growing risk. Thus, some organizations additionally aggregate the data to further obscure traces of individual behavior. This anonymize-and-aggregate process requires pre-processing and results in a coarser resolution of data, which may be less useful but more protective of privacy. Anonymization is applied in the context of retrieval and long-term storage of data for which users have already provided their explicit consent. As a general rule, organizations wishing to comply with these principles should aim to collect only data necessary and properly destroy unnecessary data as soon as possible;

(b) Purpose specification—This principle requires that the purpose for the collection of data be clearly and exclusively stated. As more data are being retained with big data, the stated

purposes for collecting and retaining data must be periodically and carefully reviewed to ensure continued compliance. Original purpose specifications might be too limiting and do not cover the newer use cases offered by big data. It is tempting for organizations to collect data now and find alternative uses for it much later. There have been a number of high-profile cases[215] involving applications collecting address book information and using this information for nondisclosed purposes. This is a typical scenario as address book information is still a manageable volume that does not require big-data-level scale. However, there are now cases of application-collecting usage and location[216] information without proper disclosure of purpose. Historically, information such as this would likely be discarded due to its volume. With big data tools available today, this information can be kept longer. Organization should clearly state and abide by their data collection purpose to avoid potential regulatory pitfalls;

(c) Use limitation - This principle generally covers disclosure rules, particularly where data must not be shared with other parties or otherwise repurposed without consent. An important action with respect to this principle is onward transfer, which means care must be taken when sharing data with third parties. The big data era has also popularized the concept of selling or monetizing data. In particular, transaction data might be anonymized, but taken together with other data from other sources, may be used to identify individual customers. It is crucial to consider that there are many readily accessible tools, algorithms, application programming interfaces (APIs) and data

[215] Schnell, Joshua; "Path Fined by FTC for Illegally Collecting Information From Children," MacGASM, 1 February 2013, www.macgasm.net/2013/02/01/path-fined-ftc-for-illegallycollecting-information-from-children/

[216] Smith, Chris; "FTC Finds Popular Flashlight App for Android Illegally Sharing Data With Advertisers," BGR, 6 December 2013, http://bgr.com/2013/12/06/flashlightapp-sharing-data-illegally-ftc/

sets that can be used for reidentification (i.e., combining Twitter postings and Netflix usage to determine customers based on what they are watching);

(d) Data quality - In the traditional data warehousing analytics space, it was required that data be structured upfront and preprocessed into appropriate data models. This provided some initial effort to validate the integrity of the data. In the new big data era, some approaches involve just storing the data as collected without preprocessing. Thus, errors may potentially remain within the stored data set that will be discovered only when the data are used. In some cases, applications are not adjusted to consider the potential "dirtiness" of the data because they were originally written for traditional data warehouses. These applications and services must be reviewed in the context of moving toward data storage and larger amounts of dirtier data;

(e) Security safeguards - This principle requires that organizations that handle personal data provide the necessary safeguards and mechanisms to ensure that personal information does not fall into the wrong hands. As organizations put more data into low-cost commodity storage (e.g., cloud) solutions, it is crucial to review the data access controls on these external systems. A good number of these solutions do not provide the same levels of access control as more mature data-warehousing products. In some solutions, controls are enforced only at the interface level, but not at the lower levels (i.e., Hadoop clusters generally have no fine-grained Hadoop distributed file system (HDFS) access controls or security for metadata). It is important that organizations implement their own controls to plug these potential compliance gaps;

(f) Openness - This principle requires information, developments and updates to be communicated to stakeholders in the most expedient manner. The implementation of this principle should be as transparent and timely as is implemented today by more mature, enterprise-class data warehouses. Organizations are encouraged to properly and promptly inform users of policy changes and developments. They are also encouraged to remind users of the consent they have already provided for the existing data sets;

(g) Individual participation—This principle emphasizes the role of the individual in the management of his/her data. The customer has the right to request personal data collected through reasonable procedures and receive a timely response. The customer also has the right to erase, rectify, complete and otherwise amend personal data. In the big data era, a good amount of data is not preprocessed in a similar fashion as traditional data warehouses. This creates a number of potential compliance problems such as difficulty erasing, retrieving or correcting data. A typical big data system is not built for interactivity, but for batch processing. This also makes the application of changes on a (presumably) static data set difficult. Organizations may find this particular requirement challenging to implement because of the potentially complex consent mechanisms required for multiple various pieces of collected information and its use. However, if they do find this challenging they might want to reconsider even handling the data in the first place because compliance is likely harder;

(h) Accountability - This principle requires that organizations that collect and store personal data be held accountable for enforcement of the other principles in this policy. This includes actions such as breach notification. The implementation of this

principle should be as implemented today by more mature, enterprise-class data warehouses.

Additional principles that are gaining acceptance and are being introduced in regulation include

(i) A priori consent and explicit opt-in - This requires that organizations ask for up-front consent and requires explicit opt-in by the individual. Organizations are encouraged to have configuration interfaces that allow their users to manage their privacy consent settings. Big data implementations normally collect data from mediation platforms or raw and unprocessed logging services, which make it difficult to remove customers who have not opted in. This may entail a substantial amount of preprocessing;

(ii) Data sovereignty -Some states have created regulation that affirms that data considered personal should not leave the territory of that state. This creates problems when implementing applications that are essentially global, but whose users may be citizens of such a state; and

(iii) Extra-personal protection - In some jurisdictions, there may be additional, distinct classes of personal information that require additional protections or controls. This class of information is normally called sensitive personal information (i.e. medical records, political views, race, religion)[217]

[217] Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu [Ph.D, CISM, CRISC, CISSP, CSSLP] ISACA Journal Volume 3 (2014) page.no. 1 to 5

CHALLENGES – IN IMPLEMENTATION OF DATA PROTECTION LAW [218]

(I) ADDRESSING GAPS IN COVERAGE

There is no single global agreement on data protection. The Council of Europe Convention 108 has had a significant real-world impact to date, and the EU Directive (soon to be upgraded to the EU GDPR) is driving international debates.

The three key gaps in coverage are as follows: (i) A significant number of countries have no data protection law at all; (ii) A significant number of countries have only partial laws, or laws that contain broad exemptions; and (iii) in some circumstances individual companies can limit the scope of their privacy promises (usually in the fine print of privacy policies). Though there is an overall strong consensus and agreement around the underlying principles of data protection.

(II) ADDRESSING NEW TECHNOLOGIES

Data protection is a dynamic field that is constantly challenged and influenced by advances in technology and innovation in business practices. The relationship between data protection and online activities

changes all the time but can be demonstrated by three recent developments: (i) Cloud computing; (ii) The Internet of Things; and (iii) Big Data analytics. Each of these challenges present an obstacle to data protection, particularly in the areas regarding the definition of 'personal data' and the management of cross-border data transfers.

(III) MANGAGING CROSS-BORDER TRANSFER RESTRICTIONS

[218] Data Protection regulation and international data flows: Implications for trade and development – United Nations Conference on Trade and Development [UNCTAD] – Chapter 6 - Conclusions

International data flows are increasingly important for trade, innovation, competition and data mobility for consumers. However, there is also a general consensus that the movement of data cannot be completely unrestricted if legitimate concerns are to be addressed. There are numerous options and arrangements are in place for managing the data flows in a way that still protects the rights of citizens. The most common mechanisms are: **(i)** allowing one-off data transfers that meet common derogations or 'tests' (for example, requirements to fulfil a contract, emergency situations, valid law enforcement requests and others); **(ii)** allowing ongoing data transfers where the target jurisdiction ensures an equivalent level of protection (this approach is used by the EU and other jurisdictions, including Israel and Japan); **(iii)** allowing data transfers where the original company agrees to be held accountable for any breaches (this is an emerging approach that appears in the APEC Privacy Framework and to a limited degree in the laws of Australia and Japan); **(iv)** allowing data transfers where the company is bound by a set of corporate rules that apply across all its activities (this approach is used in the EU BCRs, to some degree in the APEC CBPRs, and to a limited degree in national laws of, for example, Colombia and Japan); **(v)** allowing data transfers subject to a very specific legal agreement between jurisdictions (e.g. EU/U.S. agreements on transfer of airline passenger data and financial services data); and/or **(vi)** some combination of the options above (it is common for national laws and global and regional initiatives to allow individual businesses to select a mechanism that is most appropriate for them).

Although these different options for enabling cross-border data transfers are widely available, they have not been universally adopted. In some jurisdictions, specific obstacles to compatibility have emerged. Significant developments include the emergence of data localization requirements in some jurisdictions (e.g. Indonesia, Russian

Federation). While these localization requirements may seek to address certain concerns, they may also be incompatible with trade objectives.

(IV) BALANCING SURVEILLANCE AND DATA PROTECTION

It is essential that national laws and global and regional initiatives acknowledge the existence of surveillance issues and attempt to address these issues head on. Most laws and initiatives are silent on this issue, a situation that needs to change now that the extent of surveillance has been revealed. There is an emerging 'test' for achieving a balance between data protection and surveillance. There appears to be an emerging consensus around the following key principles: **(i)** the broad extent, scope and purpose of surveillance should be open, even if some operational details remain secret; **(ii)** surveillance should be limited to specific national security and law enforcement objectives; **(iii)** personal data collection during surveillance should be 'necessary and proportionate' to the purpose of the surveillance; **(iv)** surveillance activities should be subject to strong oversight and governance; **(v)** all individual data subjects should have the right to effective dispute resolution and legal redress regarding surveillance (irrespective of their nationality); **(vi)** private sector involvement in surveillance should be limited to appropriate assistance in responding to a specific request; and **(vii)** private sector organizations should be able to disclose (in broad terms) the nature and frequency of request for personal data that they receive from government, law enforcement and security agencies.

An additional test is that surveillance requests should be 'narrowly targeted'. This appears in only one key agreement to date and has not achieved the consensus that exists regarding the 'necessary and proportionate' test. Nevertheless, this addition may be adopted more widely in the future. Balancing surveillance against data protection is complex and has only emerged recently as a major issue. Most laws and international agreements have not yet addressed it in detail.

(V) STRENGTHENING ENFORCEMENT

There is a trend towards strengthening enforcement powers and sanctions in the data protection field. This is in response to a series of high profile privacy cases where existing regulatory powers have proved inadequate in the face of the massive scale and scope of the breaches. The imposition of proportionate sanctions is recognized as being important for: the target company (as a clear signal to senior management and staff regarding reform of their practices); the affected consumers (as an important form of redress for the harm they have suffered); and also, as a broader deterrent to the wider industry.

(VI) DETERMINING JURISDICTION

Determining jurisdiction has become a prominent issue in data protection regulation, partly due to the widespread data flows across borders, and partly due to the lack of a single global agreement on data protection (and the consequent fragmentation of data protection regulation). In the absence of an international agreement, jurisdiction law is complex and unsettled.

The two cases that are currently before the courts and are receiving considerable attention are U.S. v Microsoft and Belgium v Facebook). Both may have an impact on the future process for determining jurisdiction in data protection law. Some recent amendment of legislation, notably Japan's new privacy law and the EU General Data Protection Regulation, have resulted in specific provisions on jurisdiction, extending the reach of national laws through extraterritoriality provisions.

(VII) MANANGING THE COMPLIANCE BURDEN

There is a risk of data protection requirements restricting opportunities for innovation or creating unrealistic compliance burdens on business. Some data protection regulation is being criticized for being overly cumbersome or expensive to comply with, or that it creates specific compliance burdens for smaller businesses.

Examples include: (i) laws that include registration requirements, where the company has to notify the regulator of the existence of a data set; often the requirement is accompanied by a fee (these requirements appear in some but not all European national laws, with a few scattered examples in other regions); (ii) Laws that require the appointment of data protection officers (currently the subject of debate in the proposed EU General Data Protection Regulation); and (iii) requirements to establish data centres or offices in local jurisdictions.

10. REMEDIES – DATA PROTECTION [219]

In context of data protection law, the civil penalties may be calculated in a manner to ensure that the quantum of civil penalty imposed not only acts as a sanction but also acts as deterrence to

[219] White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017. [Chapter 4 - Remedies]

data controllers, which have violated obligations under the data protection law. [220]

The GDPR – EU mandates that the administrative fines imposed by a supervisory authority in each individual case must be effective, proportionate and dissuasive.[221] For specific violations, the EU GDPR prescribes an administrative fine of up to EUR 20,000,000, or in the case of an undertaking, up to four percent of the total worldwide turnover of the preceding financial year, whichever is higher.[222] In other words, administrative penalty that may be imposed on a data controller under the EU GDPR is linked to the total worldwide turnover of the preceding financial year of the defaulting data controller.

(I) ENFORCEMENT

The enforcement of data protection norms is complicated by two factors primarily: first, the application of the norms across different fields, sectors, industries and contexts and, second, the rapid pace

[220] Ibid

[221] Article 83(1), General Data Protection Regulation – European Union

[222] Article 83(5), EU GDPR, this includes instances where the data controller or data processor has infringed the basic principles for processing (including conditions for consent), data subjects' rights, and transfer of personal data to a recipient in a third country or an international organization pursuant to Articles 44-49, EU GDPR. Similar administrative fine is also prescribed where the data controller or data processor does not comply with an order of the supervisory authority. Moreover, for certain other types of infringements, Article 83(4) of the EU GDPR prescribes an administrative fine of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

of development and change in data processing technologies.[223] The enforcement model that needs to be executed, for which three different variants can be considered as follows:[224] **(i)** 'Command and control' regulation - This approach requires the State to provide legal rules or clear prescriptions for regulated entities, with no room for discretion. If these prescriptions are not followed, the State exercises its power to sanction. Where elements of a 'command and control' system are adopted, necessary features include the involvement of some governmental authority or the other, whether this involvement is through the establishment of a single, specialized agency or the creation of a federated, sectoral framework. A number of issues are raised on this point, including whether the state machinery involved should be unified, how independent it should be from governmental control and industry influence, whether it should have regional spread, what regulatory tools and forms of sanction it should have at its disposal etc. Most jurisdictions do not have data protection frameworks that are purely 'command and control' in nature and create some room for industry involvement.

(ii) Self-regulation - This approach involves private organisations complying with standards they set for themselves without any enforcement by the State.663 In a self-regulatory framework, norms become established either through market forces (such as demand for privacy from consumers), through industry standard-setting or through some limited facilitation of market transactions in the form of choice-enhancing legal rules such as information disclosure norms. Legal obligations that enhance the fairness of transactions such as notice and privacy policy requirements may require

[223] Report of the Justice AP Shah Committee, 75 (October 16, 2012)

[224] Dennis D. Hirsch, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 Seattle University Law Review 439, 440-41 (2011)

governmental enforcement machinery and do not always fit comfortably in the self-regulation rubric. The US is a good example of a jurisdiction with largely self-regulatory elements, though a few sector-specific and state-specific laws are also in place. As these rules are a threshold requirement for achieving regulatory effectiveness, they form core, substantive elements of a data protection framework and are not, appropriately, to be considered as part of the enforcement mechanism.

(iv) Co-regulation - This typically involves elements of both 'command and control' regulation and self-regulation. Co-regulation may be described as "initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards."[225] This model advocates the formulation of a general data protection statute with broad provisions complemented by "codes of practices or conduct" formulated by the industry and approved by the government or the relevant data protection authority.

(II) ADJUDICATION

Adjudication plays an integral role in the enforcement of any law as it ascertains the rights and obligations of parties involved in a dispute and prescribes the corrective actions and remedies.

[225] Ibid (describing co-regulation as "initiatives in which government and industry share responsibility for drafting and enforcing regulatory standards"); Hans-Bredow-Institut and Institute of European Media Law, 'Final Report: Study on Co-Regulation Measures in the Media Sector', 17 (June 2006)

The extant Indian legal framework, specifically the IT Act, a special class of officers called 'adjudicating officers' are appointed for hearing and adjudicating cases pertaining to violations of the provisions of the IT Act or of any rule, regulation, direction or order made thereunder.[226] The IT Act also specifies certain disputes in relation to which the adjudicating officer has the power to adjudicate.[227]

So far as the appellate mechanism under the IT Act is concerned, prior to the enactment of the Finance Act, 2017 (Finance Act), appeals from decisions of adjudicating officers lay before the CyAT set up under Section 48 of the IT Act. The CyAT, which started functioning in 2006, was set up with a specific mandate to hear appeals on matters where the jurisdiction of civil courts was barred, i.e. where the claim for injury or damage does not exceed Rs. 5 crores.[228]

Upon adjudication, the adjudicating officer under the IT Act has the power to give remedies in the form of either a civil penalty imposed upon the defaulter or grant compensation to the aggrieved individual. Section 43A of the IT Act stipulate that any person who commits the acts specified under the said provision shall be liable to pay damages by way of compensation to the person so affected.

---

[226] Section 46(1) of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922

[227] Ibid Sections 43 (Penalty and compensation for damage to computer, computer system); S.43A (Compensation for failure to protect data); S.44 (Penalty for failure to furnish information, return); and S. 45 (Residuary penalty)

[228] Ibid Section 61, IT Act

Compensation, as a remedy under Section 43A of the IT Act is extremely limited and is applicable where a body corporate fails to maintain and implement reasonable security practices and procedures.

(III) COMPENSATION

In an event of loss or damage as a result of data controller's failure to comply with the data protection principles as set out under law, a fair compensation shall be awarded to equate as a remedy.

The IT Act, albeit in a limited manner, in Section 43A, recognizes the right of an individual to claim compensation in case of a failure to protect sensitive personal data. Section 43A of the IT Act specifically stipulates that where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures[229] and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.[230]

---

[229] As per Section 43A, IT Act, 'reasonable security practices and procedures' may be specified in an agreement between the parties or may be specified under law or in the absence of such agreement or any law, such reasonable security practices and procedures as may be prescribed by the central government in consultation with such professional bodies or associations as it may deem fit.

[230] It is relevant to note that under Section 43, IT Act, if any person without the permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses or secures access to such computer, computer system or computer network, downloads, copies or extracts any data or information from the same, or provides any assistance to any person to facilitate access to the same in contravention to the provisions of the IT Act shall be liable to pay damages by way of compensation to the person so affected

Moreover, while adjudging the quantum of compensation payable under the IT Act, the adjudicating officer shall have due regard to the following factors, namely: (i) the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default; (ii) the amount of loss caused to any person as a result of the default; and (iii) the repetitive nature of the default.[231]

Under the EU GDPR[232], an individual who has suffered "material or non-material" damage as a result of the infringement of the EU GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered. It has been specified that a data controller shall be liable for the damage caused by processing which infringes the GDPR - EU and that a data processor shall only be liable where it has acted in violation of any obligation specifically applicable to data processors or has acted outside or contrary to any lawful instruction provided by the data controller. Further, court proceedings for exercising the right to receive compensation shall be brought before the competent courts in the Member States.

CONCLUSION

[231] Section 47 of The Information Technology Act of 2000 (No. 21 of 2000) Ministry of Law, Justice and Company Affairs [Legislative Department] New Delhi, Friday, June 9, 2000 / JYAISTHA 19, 1922

[232] Article 82, General Data Protection Regulation - EU

Privacy and data protection are two important components i.e. Data protection and privacy for effective functioning of cyberspace. Every individual and organization has a right to protect and preserve their personal, sensitive and commercial data and information. We have no dedicated data privacy, data protection laws in India, at the moment, but these legislations are in the pipeline to be enacted.

There are various concerns about data protection and privacy raised by consumers (civil society), businesses and governments. The challenge for data protection and privacy laws is therefore to balance these different concerns and interests, ideally in a way that does not unnecessarily hamper the scope for commerce. In order to facilitate cross-border trade online, it is also essential to seek solutions that are internationally compatible.

Data protection framework is a positive step, which will enable more control, transparency, and choice for the consumer. Therefore, it is crucial for business to create an environment which will foster trust for customers, supported by the commercial and technological framework for the use of information and consent.

The IT Act defines liabilities for violation of data confidentiality and privacy related to unauthorized access to computer, computer system, computer network or resources, unauthorized alteration, deletion, addition, modification, destruction, duplication or transmission of data, computer database. However, IT act does not cover data protection and privacy in an exhaustive manner, today one can access any information related to anyone from anywhere at any time but this poses a new threat

to private and confidential information. Globalization has given acceptance to technology in the whole

world.

In today's connected world it is very difficult to prevent information from being disseminated in public domain if someone has decided to broadcast it without using repressive methods. Data protection and privacy has been dealt within the IT (Amendment) Act, 2008 but not in an exhaustive manner. The IT Act needs to establish setting of specific standards relating to the methods and purpose of assimilation of right to privacy and personal data. To conclude it would suffice by saying that the IT Act is facing the problem of protection of data and a separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy, and the same is in pipeline to be enacted by the legislature.

The advancement in global electronic communications has created spaces in which distinct rule will evolve to keep pace with the technological invocations and ensure there is no lacuna for adjudication and effective compliance. The technological advances have created opportunities to access and use data in ways that were unimaginable even a few years ago, as well as risks to individuals, companies, and countries. Varying ideological approaches to privacy and data security in our interconnected digital world complicate the already difficult task of balancing innovation with reasonable protections. The corporates should ensure that the data processed should be minimal and necessary for the purposes for which such data is sought and other compatible purposes.

Data protection laws across jurisdictions have defined the term 'processing' in various ways. It is important to formulate an inclusive

definition of processing to identify all operations, which may be performed on personal data, and consequently be subject to the data protection law.

The power of the State to prescribe and enforce laws is governed by the rules of jurisdiction in international law. Data protection laws challenge this traditional conception as the act of processing data/information could occur across jurisdictions. In this context, it is necessary to determine the applicability of the proposed data protection law. The possible outcomes to overcome the jurisdictional challenge to cover cases where wholly or partly happens in India irrespective of the status of the entity and regulate entities which offer goods or services in India even though they may not have a presence in India.

Therefore, the Data protection framework needs to be based on principles which makes it flexible to take into account the ever-changing nature of technological advancements and accordingly change standards of compliance. The framework should have differential obligations to create legitimate state aims for both private sector entities and government.

In digital era, privacy must be a priority. Is it just me, or is secret blanket surveillance obscenely outrageous?

– Al Gore

BIBLIOGRAPHY

TEXTBOOKS

1. Fundamentals of Database Systems by Ramez Elmasri, Shamkant B Navathe [Published by Addison-Wesley]
2. Introduction to the Structural Elements of Cyberspace by Elihu Zimet and Edward Skoudis [Chapter 4] Available at: http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-04.pdf

ARTICLES

1. W. K. Khong, National and International Developments on Copyright and Rights in Databases [6 MALYSIAN J LIB. & INFO. SCIENCE 71, 72 (2001)]
2. Brown Mart, Bryan Robert M & Conley John M, Database Protection in a Digital World, Richmond Journal of Law & Technology, 6 (1) (1992) Pg. 2-10
3. Emerging Challenge: Security and Safety in Cyberspace by Richard O Hundley and Robert H Anderson Published by RAND Corporation (1997
4. Laura DeNardis, The Global War for Internet Governance (New Haven and London: Yale University Press, 2014) 227
5. Policy Brief - Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance by The Hague Institute for Global Justice [November 2015]
6. Enrico Calandro and Nicolo Zingales, "Stakeholders' involvement and participation in the Internet governance ecosystem from an African perspective," (Working Paper for the Global Governance Reform Initiative Project of The Hague Institute for Global Justice, 2015)
7. Lee Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic, and Limits' 2 (Kluwer Law International: The Hague/London/New York, 2002)
8. Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).
9. Maria Tzanou, 'Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right,' 3(2) International Data Privacy Law 88 (1 May 2013).

10. Privacy and Data Protection in Cyberspace in Indian Environment by Shrikant Ardhapurkar, Tanu Srivastava, Swati Sharma, Mr. Vijay Chaurasiya, and Mr. Abhiskeh Vaish [International Journal of Engineering Science and Technology Vol. 2(5), 2010 Page 942-951]
11. Francois Nawrot, Katarzyna Syska and Przemyslaw Switalski, "Horizontal application of fundamental rights – Right to privacy on the internet", 9 th Annual European Constitutionalism Seminar (May 2010)
12. Christina P. Moniodis, "Moving from Nixon to NASA: Privacy 's Second Strand- A Right to Informational Privacy", Yale Journal of Law and Technology (2012), Vol. 15 (1),
13. Use of Object-Oriented Concepts in Databases for Effective Mining by Ajita Satheesh and Dr. Ravindra Patel [International Journal on Computer Science and Engineering – Vol.1(3), 2009,
14. Yvonne McDermott, "Conceptualizing the right to data protection in an era of Big Data", Big Data and Society (2017
15. Richard A. Posner, "Privacy, Surveillance, and Law", The University of Chicago Law Review (2008), Vol.75
16. Privacy and Data Protection in India: A Critical Assessment by Shiv Shankar Singh [Journal of Indian Law Institute Volume.53:4 Page No. 663-677]
17. Overview of Data Privacy Laws in India and Aspects of Data Protection that account when establishing a business in India by Supratim Chakraborty and Aritri Roy Chowdhury
18. Working with Last Mile Data Protection in India by Arun Sukumar [Asie. Visions. No. 96, Ifri – Centre for Asian Studies, November, 2017] page.no.5-21
19. White Paper on the Committee of Experts on a Data Protection Framework for India, released on November 27, 2017
20. The Digital Universe of Opportunities: Rich Data and the Increasing Values of the Internet of Things', EMC Digital Universe with Research and Analysis by IDC (April 2014)
21. Big data: Changing the Way Businesses Operate and Compete', Ernst & Young (April 2014)
22. Ryan Moshell, 'And then there was one: The outlook for a self-regulatory United States amidst a global trend towards comprehensive data protection framework', 37 Texas Tech Law Review 357 (2005).

23. Tom Goodwin, 'The Battle is for Customer Interface', TechCrunch (3 March 2015 available at: https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/
24. Helen Nissenbaum, 'Privacy in Context-Technology, Policy, and the Integrity of Social Life', 36, (Stanford University Press, 2010).
25. Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', 52 Stanford Law Review 1315 (1999).
26. J.B. Schafer, J.A. Konstan, and J. Reidl, "E-Commerce Recommendation Applications," Data Mining and Knowledge Discovery, Kluwer Academic, 2001, pp. 115-153.
27. P. Resnick et al., "GroupLens: An Open Architecture for Collaborative Filtering of Netnews," Proc. ACM 1994 Conf. Computer Supported Cooperative Work, ACM Press, 1994, pp. 175-186
28. Industry Report – Amazon.com Recommendations (Item to Item Collaborative Filtering) by Gren Linden, Brent Smith, and Jeremy York – Published by the IEEE Computer Society – January – February, 2003 [Recommendation Alogrithms]
29. Jordi Soria-Comas and Josep Domingo-Ferrer, 'Big Data Privacy: Challenges to Privacy Principles and Models', 1(1) Data Science and Engineering (March 2016)
30. Avner Levin and Mary Jo Nicholson, 'Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground', 2(2) University of Ottawa Law & Technology Journal, 357 (2005).
31. Data Privacy and Big Data – Compliance Issues and Considerations by William Emmanuel Yu ISACA Journal Volume 3 (2014) page.no. 1 to 5

STATUTES AND CONVENTION

1. The Information Technology Act of 2000 (No. 21 of 2000)
2. Copyright, Designs, and Patents Act, 1998
3. EU General Data Protection Regulation, 2016 (Regulation (EU) 2016/679)
4. UNCITRAL - Model Law on Electronic Commerce wit Guide to Enactment, 1996 [United Nations Publication Sales No.E.99. V.4]

OTHER SOURCES

1. NETmundial Multistakeholder Statement, - Global Multistakeholder Meeting on the Future of Internet Governance, accessed August 11, 2015 [http://netmundial.br/wp-content/uploads/2014/04/ NETmundial-Multistakeholder-Document.pdf]
2. Press release 45/2017 available at http://trai.gov.in/sites/default/files/PR_No.45of2017.pdf
3. United Nations General Assembly [A/RES /51/162 dated January 30th, 1997]
4. Digital India – Power to Empower [Ministry of Electronics & Formation Technology Government of India] http://digitalindia.gov.in/content/about-programme
5. Office Memorandum No.3 (6)/2017 – CLES (Ministry of Electronics & Information Technology – Government of India) – Constitution of a Committee of Experts to deliberate on a data protection framework for India

CITATION

1. Justice K S Puttaswamy (Retd) &Anr v. Union of India & Others [AIR 2017 SC 4161]
2. Karmanya Singh Sareen & Another v. Union of India & Others 2016 (68) PTC 486 (Del)

NEWSPAPER ARTICLE

1. Reetika Khera, 'The Different Ways in Which Aadhaar Infringes on Privacy', The Wire (19 July 2017), available at https://thewire.in/159092/privacy-aadhaar-supreme-court/
2. Jean Dreze, 'Hello Aadhaar, Goodbye Privacy', The Wire (24 March, 2017) available at https://thewire.in/118655/hello-aadhaar-goodbye-privacy/
3. Subhashis Banerjee *et al.,* A Computer Science Perspective: Privacy and Security of Aadhaar, 52(37) Economic & Political Weekly (16 September 2017).