PART I
CONTEXT-SETTING

1. A Digital India in a Digital World

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.[1] Much of that new information will consist of personal details relating to individuals, including information relating to the products they have purchased, the places they have travelled to and data which is produced from "smart devices" connected to the Internet.

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. Proprietary algorithms are being developed to comb this data for trends, patterns and hidden nuances by businesses.[2] Many of these activities are beneficial to individuals, allowing their problems to be addressed with greater accuracy.[3] For instance, the analysis of very large and complex sets of data is done today through Big Data analytics. Employing such analytics enables organisations and governments to gain remarkable insights into areas such as health, food security, intelligent transport systems, energy efficiency and urban planning.[4] This is nothing short of a digital revolution.

This digital revolution has permeated India as well. Recognising its significance, and that it promises to bring large disruptions in almost all sectors of society, the Government of India has envisaged and implemented the "Digital India" initiative. This initiative involves the incorporation of digitisation in governance; healthcare and educational services; cashless economy and digital transactions; transparency in bureaucracy; fair and quick distribution of

[1] '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.htm, (last accessed 4 November 2017).

[2] 'Big data: Changing the Way Businesses Operate and Compete', Ernst & Young (April 2014), available at:http://www.ey.com/Publication/vwLUAssets/EY_-_Big_data:_changing_the_way_businesses_operate/%24FILE/EY-Insights-on-GRC-Big-data.pdf, (last accessed November 20, 2017).

[3] Roger Parloff, 'Why Deep Learning is Suddenly Changing your Life', Fortune Magazine (28 September 2016), available at: http://fortune.com/ai-artificial-intelligence-deep-machine-learning/, (last accessed 3 November 2017).

[4] European Commission, 'European Data Protection Reform and Big Data: Factsheet', (2016), available at: http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf, (last accessed 4 November 2017).

welfare schemes etc to empower citizens.[5] With nearly 450 million Internet users and a growth rate of 7-8%, India is well on the path to becoming a digital economy, which has a large market for global players.[6] This digital economy is expected to generate new market growth opportunities and jobs in the coming 40-50 years.[7]

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.[8] As has been noted by the Supreme Court in *Puttaswamy*[9]:

> "*'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.*"[10]

Something as simple as hailing a taxi now involves the use of a mobile application which collects and uses various types of data, such as the user's financial information, her real-time location, and information concerning her previous trips. Data is fundamentally transforming the way individuals do business, how they communicate, and how they make their decisions. Businesses are now building vast databases of consumer preferences and behaviour. Information can be compressed, sorted, manipulated, discovered and interpreted as never before, and can thus be more easily transformed into useful knowledge.[11] 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.[12] Such

---

[5] Press Information Bureau, 'Digital India – A programme to transform India into digital empowered society and knowledge economy' (20 August 2014), available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926 (last accessed 16 November 2017).

[6] Arushi Chopra, 'Number of Internet users in India could cross 450 million by June: report', LiveMint (2 March 2017), available at: http://www.livemint.com/Industry/QWzIOYEsfQJknXhC3HiuVI/Number-of-Internet-users-in-India-could-cross-450-million-by.html, (last accessed 5 November 2017).

[7] Ranjan Guha, 'Digital Evolution in India', Business Today (29 August 2017), available at: http://www.businesstoday.in/opinion/columns/digital-evolution-in-india/story/259227.html, (last accessed 4 November 2017).

[8] 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).

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1.

[10] 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/ (last accessed 14 November 2017) cited in *Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1, Per S.K. Kaul, J. at paragraph 17.

[11] Helen Nissenbaum, 'Privacy in Context-Technology, Policy, and the Integrity of Social Life', 36, (Stanford University Press, 2010).

[12] Joel Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace', 52 Stanford Law Review 1315 (1999).

information can then be used to create customised user profiles, 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.[13]

There are a large number of benefits to be gained by collecting and analysing personal data from individuals. Pooled datasets allow quicker detection of trends and accurate targeting. For instance, in the healthcare sector, by collecting and analysing large data sets of individual's health records and previous hospital visits, health care providers could make diagnostic predictions and treatment suggestions;[14] an individual's personal locational data could be used for monitoring traffic and improving driving conditions on the road;[15] banks can use Big Data techniques to improve fraud detection;[16] insurers can make the process of applying for insurance easier by using valuable knowledge gleaned from pooled datasets.[17]

At the same time, the state processes personal data for a plethora of purposes, and is arguably its largest processor. 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, etc. 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.[18]

Thus both the public and the private sector are collecting and using personal data at an unprecedented scale and for multifarious purposes. While data can be put to beneficial use, the unregulated and arbitrary use of data, especially personal data, has raised concerns regarding the privacy and autonomy of an individual. Some of the concerns relate to

---

[13] For an illustrative example, see Greg Linden *et al.*, 'Amazon.com Recommendations: Item to Item Collaborative Filtering', University of Maryland: Department of Computer Science, available at: https://www.cs.umd.edu/~samir/498/Amazon-Recommendations.pdf (last accessed 5 November 2017).

[14] Clemens Suter-Crazzolara, 'Big Data And The Journey To Personalized Medicine', Forbes (17 November 2015), available at: https://www.forbes.com/sites/sap/2015/11/17/big-data-and-the-journey-to-personalized-medicine/#7865d751b0ee, (last accessed 20 November 2017).

[15] Matthew Sparks, 'GPS Big Data: making cities safer for cyclists', The Telegraph (9 May 2014), available at: http://www.telegraph.co.uk/technology/news/10818956/GPS-big-data-making-cities-safer-for-cyclists.html, (last accessed 5 November 2017).

[16] Jacomo Corbo *et al.*, 'Applying analytics in financial institutions' fight against fraud', McKinsey and Company (April 2017), available at:https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/applying-analytics-in-financial-institutions-fight-against-fraud, (last accessed 5 November 2017).

[17] Information Commissioner's Office (UK), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[18] 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 (last accessed 5 November 2017); 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 (last accessed 16 November 2017); 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/internet-governance/blog/the-design-technology-behind-india2019s-surveillance-programmes (last accessed 16 November 2017).

centralisation of databases, profiling of individuals, increased surveillance and a consequent erosion of individual autonomy. This was also the subject matter of the landmark judgement of the Supreme Court in *Puttaswamy*, which recognised the right to privacy as a fundamental right.[19] The Supreme Court stated that the "right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution and as a part of the freedoms guaranteed by Part III of the Constitution".[20] Further, it went on to recognise informational privacy as a facet of the right to privacy and directed the Union Government to put in place a robust data protection regime to ensure protection against the dangers posed to an individual's privacy by state and non-state actors in the information age.[21]

In this light, in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India.

2. Data Protection: Genesis and Rationale

(i) Data Protection and the Value of Privacy

Data protection principles are designed to protect the personal information of individuals by restricting how such information can be collected, used and disclosed.[22] As a legal right, it has developed in many jurisdictions because of the emergence of a wide range of issues related to personal information being processed through "automated" means.[23] In order to understand these issues, it is important to examine how the usage of personal information is an important activity in society as it not only reaps many benefits but is also capable of causing considerable harm. The need for data protection thus arises out of the need to prevent such harms, and hinges on the question of who should be permitted to use personal information and how.

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).[24] The concept of data protection is primarily linked with the idea of informational privacy,[25] though given the deeply pervasive nature of technology, its impact on decisional privacy and spatial privacy is also discernible. Though privacy is popularly associated with seclusion or secrecy, as a legal right, it is understood as a question of control over personal information.

---

[19] 2017 (10) SCALE 1.
[20] 2017 (10) SCALE 1.
[21] 2017 (10) SCALE 1.
[22] Lee Bygrave, 'Data Protection Law: Approaching Its Rationale, Logic, and Limits' 2 (Kluwer Law International: The Hague/London/New York, 2002).
[23] *See* definition of 'processing' under Article 4 (2) of the EU General Data Protection Regulation, 2016 (Regulation (EU) 2016/679).
[24] Jerry Kang, 'Information Privacy in Cyberspace Transactions', 50 Stanford Law Review 1193, 1202-03 (April 1998).
[25] 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).

Privacy is a complex concept that has been difficult to define. In many circumstances, the harms that arise from violations of privacy are difficult to identify because very often they are intangible. Despite its amorphous nature, there are a number of reasons why protecting privacy is considered valuable. The protection of privacy permits individuals to plan and carry out their lives without unnecessary intrusion.[26] Informational privacy is often understood as the freedom of individuals "to determine for themselves when, how, and to what extent information about them is communicated to others"[27] and this freedom allows for individuals to protect themselves from harm. However, not all information about an individual is necessarily private and deserving of protection. It is for a legal framework to determine where affording such freedom is appropriate and where it is not.

Certain aspects related to an individual are considered especially central to their identity, such as their bodies, their sexuality, or their ability to develop their own distinct personalities.[28] Privacy is also valued where it legitimately protects an individual's reputation. Disclosure of certain kinds of inflammatory and sensitive information, even where the information is true, unfairly results in the stereotyping and pre-judging of individual.[29] In some circumstances, information about an individual (such as their race, religion, caste etc.) can be used to discriminate against them. There are also some actions of the state which may threaten an individual's privacy. For instance, surveillance activities by government or private organisations can disrupt peace of mind and create chilling effects by making people conform to societal expectations.[30]

However, it is not possible to conclusively demarcate all the aspects requiring protection in this manner as the relevant concerns arise in varying contexts. Privacy does not arise only in some special, unchanging space like the home or the family but also in various situations including in public spaces. Different norms of privacy can exist in different spheres of life.[31] For example, an individual may be willing to disclose certain things to a doctor or psychologist that she would not even tell her spouse or friends. Rules of data protection and privacy are designed in such a way that they allow individuals the freedom to determine how their personal information will be collected, used and disclosed. This is because individuals themselves are best equipped to understand how they will be benefited or harmed in the many unique contexts which involve their personal information.

Privacy laws are not identical in form to any other existing fields of law like property, copyright or tort law, though there are some similarities.[32] For example, laws on defamation

[26] *Time, Inc. v. Hill*, 385 U.S. 374, 413 (1967) (Fortas, J., dissenting); *Doe v. Bolton*, 410 U.S. 179, 213 (1973) (Douglas, J., concurring)
[27] Alan Westin, 'Privacy and Freedom', 7, (Atheneum, 1967).
[28] Stanley I. Benn, 'Privacy, Freedom, and Respect for Persons,' in 'Nomos XIII: Privacy', 26 (J. Ronald Pennock and J.W. Chapman *eds*., 1971).
[29] Jeffrey Rosen, 'The Unwanted Gaze: The Destruction of Privacy in America' (Random House, 2000).
[30] Neil M. Richards, 'The Dangers of Surveillance,' 126 (7) Harvard Law Review 1934, 1950 (20 May 2013).
[31] Helen Nissenbaum, 'Privacy as Contextual Integrity', 79 Washington Law Review 119 (2004).
[32] Daniel Solove, 'Conceptualizing Privacy', 90 (4) California Law Review 1088-89, 1100-02, 1112-13, 1130-31, (July 2002).

generally prohibit disclosure of personal information only if it is false. Privacy, on the other hand, would even protect against disclosure of truthful personal information.[33] The source and application of privacy has not been confined to constitutional law, criminal procedure or evidentiary rules. Defining appropriate rules as to how personal information should be distributed thus requires *sui generis* concepts and tools. One important aspect that arises in the unique framework of privacy is the method by which we identify harms. These can be subjective or objective.[34] A subjective harm is one where an individual has not actually suffered any tangible loss but anticipates such loss after personal information is collected. The uncertainty, anxiety and fear of potential observation are the identified harms in this situation. On the other hand, objective harms are separately identified when the use of one's personal information actually results in some damage, whether through loss of reputation or through some other change in the treatment of the individual by society. Data protection must account for both these kinds of harms which arise as a result of unregulated collection and use of personal information.

(ii) The Evolution of Privacy Principles

The 1970s witnessed increasing use of automated data systems containing personal information about individuals.[35] To address concerns surrounding this, the Government of the United States appointed an Advisory Committee in the Department of Health, Education and Welfare (HEW Committee) to examine the various legal and technological issues raised vis-a-vis increasingly automated processing of data. The HEW Committee went on to issue a landmark report titled '*Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems',* which recommended that the United States Congress develop a Code of Fair Information Practices based on Fair Information Practices Principles (FIPPS).[36] The FIPPS are a set of principles which prescribe how data should be handled, stored and managed to maintain fairness, privacy and security in a rapidly growing global technology environment.[37] FIPPS are now deemed to be the bedrock of modern data protection laws across the world.[38]

---

[33] Samuel Warren and Louis Brandeis, 'The Right to Privacy,' 4(5) Harvard Law Review 193 (15 December 1890).
[34] Ryan M. Calo, 'The Boundaries of Privacy Harm', 86 Indiana Law Journal 1131, 1142-43 (2011).
[35] Robert Gellman, 'Fair Information Practices: A Brief History' (April 10, 2017), available at: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (last accessed 31 October 2017).
[36] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).
[37] Pam Dixon, 'A brief introduction to fair information practice principles', World Privacy Forum (2006), available at: https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (last accessed 31 October 2017).
[38] The FIPPS are as follows:

1. There must be no personal-data record-keeping systems whose very existence is secret.
2. There must be a way for an individual, to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.

The FIPPS were soon followed by the Organisation for Economic Cooperation and Development Privacy Guidelines (OECD Guidelines) in the 1980s.[39] The OECD Guidelines were significantly inspired by the FIPPS and were intended to provide a framework for harmonising national privacy legislations amongst OECD members, while upholding human rights, and preventing interruptions in international flows of data.[40] The OECD Guidelines are deemed to be the first internationally agreed upon statement of core information privacy principles and have considerably influenced data protection frameworks around the world.[41]

The 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 Australia's Privacy Act, 1988 (Privacy Act), New Zealand's Privacy Act, 1993 and Japan's Protection of Personal Information Act, 2003.[42] However, despite the popularity that traditional privacy principles have enjoyed, they have come under considerable scrutiny in recent times.[43]

It has been argued that traditional privacy principles may not be well-suited to address the challenges posed by the dramatic increase in the volume and use of personal data, advances in computing, and global flows of data. As a consequence of these concerns, an expert group was constituted to revise and modernise the OECD Guidelines. The OECD Guidelines as updated in 2013 (2013 OECD Guidelines) are the product of this attempt. While the 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,[44] data security breach notification[45] which oblige data controllers to

---

5. Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

[39] 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 (last accessed 31 October 2017).

[40] 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 (last accessed 31 October 2017).

[41] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[42] 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 (last accessed 31 October 2017).

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

[44] 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 (last accessed 31 October 2017).

inform individuals/authorities of a security breach and establishment and maintenance of privacy enforcement authorities.[46] Further cross-border flows of data[47] and international cooperation to improve global interoperability of privacy frameworks have been recognised as essential for a global data economy.[48]

The 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.[49] Presently, corporations possess data that has been generated or collected from a wide variety of sources. Such data may include financial data, employee data and customer data. It may be relevant to note that at the time when these guidelines originated, data processing, including collection activities were more linear and easier to define. However, now the situation has changed with data being collected and used in ways not envisaged at the time these principles were developed. We have, as a consequence, been ushered into the era of modern technologies and Big Data analytics. While Big Data does not have a precise definition, it can be understood as essentially involving gathering large quantities of data and applying innovative technology (such as predictive analysis) to them to extract knowledge.[50] Big Data is usually characterised by 3 Vs, namely 'volume' as in massive datasets, 'velocity' which relates to real time data, and 'variety' which relates to different sources of data.[51] Other technological developments such as artificial intelligence,[52] machine learning[53], the Internet of Things[54] are all part of the Big Data ecosystem and their use is becoming increasingly commonplace.

---

[45] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[46] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[47] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[48] OECD, 'Thirty Years After: The OECD Privacy Guidelines' (2011), available at: http://www.oecd.org/sti/ieconomy/49710223.pdf (last accessed 31 October 2017).

[49] 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 (last accessed 31 October 2017).

[50] 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).

[51] Information Commissioner's Office (UK), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[52] Artificial Intelligence pertains to 'giving computers behaviours which would be thought intelligence in human beings'. *See* The Society for the Study of Artificial Intelligence and Simulation of Behaviour, 'What is Artificial Intelligence', available at: http://www.aisb.org.uk/public-engagement/what-is-ai, (last accessed 3 November 2017); *See generally* Information Commissioner's Office (UK), 'Big Data, Artificial Intelligence, Machine Learning and Data Protection', available at: https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/ (last accessed 31 October 2017).

[53] Machine Learning is defined as: 'the set of techniques that allow computers to think by creating mathematical algorithms based on accumulated data'. *See* Deb Miller Landau, 'Artificial Intelligence and Machine Learning: How Computers Learn', IQ Intel (17 August 2016), available at: https://iq.intel.com/artificial-intelligence-and-machine-learning/,(last accessed 3 November 2017).

[54] 'The concept of the Internet of Things or IoT refers to an infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.', *See* Article 29 Data Protection Working Party Opinion, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things', European Commission (16

In light of these developments, the biggest challenge in regulating emerging technologies such as Big Data, artificial intelligence and the Internet of Things, lies in the fact that they may operate outside the framework of traditional privacy principles. These principles, as they were originally envisaged, were designed to protect a single static data set.[55] Thus, it was possible to limit the collection of data to satisfy a particular purpose. However, this limited activity may no longer hold true with respect to current data processing activities. For instance, given that Big Data involves the processing of large data sets, usually the source of such data may not be directly from the individual, and consent may not be as relevant. Further, data may be generated as a by-product of a transaction or obtained by a service provider in return for a free service (such as free email accounts, social networks etc.) or obtained as a consequence of accessing a service (such as use of GPS navigation), and it may not be possible to specify the purpose for which personal data is collected at the time of collection.[56]

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.[57] 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.[58] 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.[59] Additionally, technologies such as the Internet of Things relies on continuous collection of personal information from the users of "smart devices", which may then be interpreted to provide unique services.[60] 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

---

September 2014), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, (last accessed 3 November 2017).

[55] 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 (last accessed 31 October 2017).

[56] 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).

[57] 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).

[58] 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/ (last accessed 1 November 2017).

[59] 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 (last accessed 31 October 2017).

[60] 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/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf, (last accessed 3 November 2017).

of emerging technologies, alternatives to traditional privacy principles have thus been suggested that require careful scrutiny.[61]

Since technologies such as Big Data, the Internet of Things and Artificial Intelligence are here to stay and hold out the promise of welfare and innovation, India will have to develop a data protection law which can successfully address the issues relating to these technologies, so as to ensure a balance between innovation and privacy. Whether this involves a reiteration of traditional privacy principles, an alternative approach based on newer *ex ante* forms of regulation or a hybrid model, will have to be determined carefully.

3. Comparative Approaches to Data Protection

In determining, India's approach to data protection, it will be instructive to look at practices followed in other jurisdictions, particularly recent models that have emerged. A perusal of foreign jurisdictions demonstrates that there are two distinct models in the field of data protection. The European Union or EU model and others similar to it, provide for a comprehensive data protection law couched in the rights based approach; and the American marketplace model has sector specific data protection laws. This is because of the distinct conceptual basis for privacy in each jurisdiction.[62] The two approaches towards data protection are discussed briefly below:[63]

European Union

In EU, the right to privacy is a fundamental right which seeks to protect an individual's dignity.[64] The European Charter of Fundamental Rights (EU Charter) recognises the right to privacy as well as the right to protection of personal data, in Article 7[65] and Article 8,[66] respectively. The first principal EU legal instrument on data protection was the Data Protection Directive.[67] The Data Protection Directive has been significantly inspired by the

[61] 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 (last accessed 31 October 2017).

[62] 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).

[63] In this part, the regulatory approach towards data protection will be discussed – specific practices will be discussed in detail under the section *International Practices* in the White Paper.

[64] 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).

[65] Respect for private and family life - Everyone has the right to respect for his or her private and family life, home and communications

[66] 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.
3. Compliance with these rules shall be subject to control by an independent authority.

[67] 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, (last accessed 4 November 2017).

OECD Guidelines,[68] 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.[69] The Data Protection 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.[70] The rapidly changing data landscape led the EU to update its regulatory environment on data protection.[71] 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 data protection laws in the world[72] 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, etc.[73] Similarly, it continues to recognise and enforce the core data protection principles recognised in the OECD Guidelines.[74] 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.[75] 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.[76] 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,[77] data minimisation,[78] data quality,[79] security safeguards,[80] etc.

---

[68] 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 (last accessed 31 October 2017).

[69] 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, (last accessed 4 November 2017).

[70] The EU GDPR, 'How did we get here?', available at http://www.eugdpr.org/how-did-we-get-here-.html (last accessed 4 November 2017.)

[71] The EU GDPR, 'How did we get here?', available at http://www.eugdpr.org/how-did-we-get-here-.html (last accessed 4 November 2017).

[72] DLA Piper, 'EU General Data Protection Regulation' available at https://www.dlapiper.com/en/asiapacific/focus/eu-data-protection-regulation/home (last accessed 5 November 2017).

[73] Article 23, EU GDPR.

[74] 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 (last accessed 31 October 2017).

[75] 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).

[76] Article 9, EU GDPR

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

[78] Article 5(1)(c), EU GDPR.

Further, an individual continues to exercise extensive control over her data post collection. This is enabled by a gamut of individual participation rights guaranteed under the law. These includes: the right to confirm if data about oneself is being collected[81], the right to access data[82], the right to rectification of data[83], the right to data portability[84], the right to restrict processing[85], the right to erasure[86], the right to object to processing[87], the right to object to processing for the purpose of direct marketing[88], the right to object to automated decisions[89].

The EU model also envisages an independent supervising authority (a regulator) who is armed with an array of functions and powers.[90] 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.[91] Significant powers of imposing penalties are vested in the regulator to ensure effective compliance.

The EU model appears to be the preferred mode in several countries who have adopted data protection legislations recently.[92] A variation of this law, which may be described as a co-regulatory model, was earlier adopted in Australia in the form of the Privacy Act and in Canada in the form of the Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA). In both Australia and Canada, co-regulatory hybrid models involve the cooperation of industry and government.[93]

United States

On the contrary, in the US, privacy protection is essentially a "liberty protection" i.e. protection of the personal space from government.[94] Thus, the American understanding of the "right to be let alone" has come to represent a desire for as little government intrusion as possible. [95] 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

[79] Article 5(1)(d), EU GDPR.
[80] Article 5(1)(f), EU GDPR.
[81] Article 15(1), EU GDPR.
[82] Article 15, EU GDPR.
[83] Article 16, EU GDPR.
[84] Article 20, EU GDPR
[85] Article 19, EU GDPR.
[86] Article 18, EU GDPR.
[87] Article 21, EU GDPR.
[88] Article 21(2), EU GDPR.
[89] Article 22, EU GDPR.
[90] Articles 4(21) and 51, EU GDPR.
[91] Section 51, EU GDPR.
[92] *See* for example, South African Law Reform Commission, 'Privacy and Data Protection' Discussion Paper 109, Project 124 (October 2005), available at: http://www.justice.gov.za/salrc/dpapers/dp109.pdf; (last accessed 2 November 2017).
[93] 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).
[94] 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).
[95] 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).

Constitution – the right against unreasonable searches and seizures. US courts however, have collectively recognised a right to privacy by piecing together the limited privacy protections reflected in the First, Fourth, Fifth and Fourteenth Amendments to the US Constitution.[96]

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 address the use, collection and disclosure of data in the US. [97] Instead, there is limited sector specific regulation.[98]

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[99] 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, etc. 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) etc. In addition, States have their own data protection laws.

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[100] which has the responsibility to ensure consumer privacy enforcement. It does this by bringing enforcement actions against 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",[101] 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.[102]

Further, US statutes and regulations have also tended to focus on "notice and consent". For instance, Title V of the GLB Act has only three substantive restrictions on processing of

[96] *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 (2005).
[97] Joel R Reidenberg, 'Data Protection in the Private Sector in the United States' 3 International Yearbook of Law Computers and Technology (1993).
[98] 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).
[99] 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 (2005).
[100] FTC, 'What we do', available at https://www.ftc.gov/about-ftc/what-we-do (last accessed 4 November 2017)
[101] 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 (last accessed 4 November 2017).
[102] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).

personal information and instead emphasises on procedural requirements, specifically, the need for institutions to "clearly and conspicuously" provide consumers with notice pertaining to its disclosure practices and an opportunity to opt out of such disclosure.[103] Another example is the rules pertaining to privacy of personal health information under the HIPAA. The HIPAA essentially envisages three types of notice and consent requirements.[104] Such emphasis on notice and consent is the *status quo* of data protection laws in the US.

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,[105] as opposed to the rights-centric culture of the EU.

4. Data Protection in India

Drafting a data protection law for India is not a greenfield exercise. Though piecemeal, several legislative developments and judicial pronouncements are relevant for determining the contours of such a law.

(i) Judicial Developments on Right to Privacy

The Supreme Court in *Puttaswamy* overruled its previous judgments of *M.P. Sharma v. Satish Chandra* (*M.P. Sharma*)[106] and *Kharak Singh v. State of Uttar Pradesh* (*Kharak Singh*)[107] which appeared to observe that there was no fundamental right to privacy enshrined in the Constitution of India. By doing so, it upheld several precedents following *Kharak Singh*, which had recognised a right to privacy flowing from Article 21 of the Constitution of India.[108]

The Supreme Court in *M.P. Sharma* examined whether the constitutionality of search and seizure of documents pursuant to a FIR would violate the right to privacy. A majority decision by an eight-judge Constitution bench observed that the right to privacy was not a fundamental right under the Constitution.

Subsequently, in *Kharak Singh,* the issue at hand was whether regular surveillance by police authorities amounted to an infringement of constitutionally guaranteed fundamental rights. A Constitution bench of six judges analysed this issue in the backdrop of the validity of the regulations governing the Uttar Pradesh police which legalised secret picketing, domiciliary

[103] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).
[104] Fred H. Cate, 'Failure of Fair Information Principles', in 'Consumer Protection in the Age of Information Economy', (Jane K. Winn *ed.*, Routledge, 2006).
[105] 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).
[106] *M.P. Sharma v. Satish Chandra*, (1954) SCR 1077.
[107] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332.
[108] For illustrative examples see, *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148; *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632; *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

visits at night and regular surveillance., The Supreme Court struck down night-time domiciliary visits by the police as violative of 'ordered liberty'.[109] Further, the Supreme Court held that Article 21 of the Constitution of India is the repository of residuary personal rights and it recognised the common law right to privacy. However, the Court observed that privacy is not a guaranteed fundamental right. It must be noted though, dissenting judge, Justice Subba Rao, opined that even though the right to privacy was not expressly recognised as a fundamental right, it was an essential ingredient of personal liberty under Article 21 and thus fundamental.

Following this approach of Justice Subba Rao, the nine-judge bench of the Supreme Court in *Puttaswamy* recognised the right to privacy as an intrinsic part of the fundamental right to life and personal liberty under Article 21 of the Constitution of India in particular, and in all fundamental rights in Part III which protect freedoms in general, and overruled the aforementioned judgments to this extent.[110] Notably, it was held that the Constitution of India must evolve with the circumstances of time to meet the challenges thrown up in a democratic order governed by the rule of law and that the meaning of the Constitution of India cannot be frozen on the perspectives present when it was adopted.

The right to privacy was grounded in rights to freedom under both Article 21 and Article 19 of the Constitution of India encompassing freedom of the body as well as the mind. It was held that "privacy facilitates freedom and is intrinsic to the exercise of liberty"[111] and examples of the freedoms enshrined under Article 25, Article 26 and Article 28(3) of the Constitution of India were given to show how the right to privacy was necessary to exercise all the aforementioned rights.[112] The approach of the Supreme Court in *Kharak Singh* and *A.K. Gopalan v. State of Madras*[113] of putting the freedoms given under Part III of the Constitution of India under distinct compartments was also rejected. Instead, it was held that that these rights are overlapping and the restriction of one freedom affects the other, as was also held previously in the *Maneka*[114] and *Cooper*[115] judgments.[116] Therefore, a law restricting a freedom under Article 21 of the Constitution of India would also have to meet the reasonableness requirements under Article 19 and Article 14 of the Constitution of India.[117]

The Supreme Court acknowledged that the concept of the right to privacy, as seen from jurisprudence in India and abroad has evolved from the basic right to be let alone, to a range of negative and poistive rights. Thus it now includes 'the right to abort a foetus; rights as to procreation, contraception, general family relationships, child rearing, education, data

[109] *Kharak Singh v. State of Uttar Pradesh*, (1964) 1 SCR 332. Also discussed: Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[110] Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[111] Per D.Y. Chandrachud, J. at paragraph 169.
[112] Per S.A. Bobde, J. at paragraph 32.
[113] *A.K. Gopalan v. State of Madras,* AIR 1950 SC 27
[114] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.
[115] *Rustom Cavasji Cooper v. Union of India*, (1970) 1 SCC 248.
[116] Per D.Y. Chandrachud, J. at paragraph 164; per S.A. Bobde at Paragraph 7.
[117] Per D.Y. Chandrachud, J. at paragraph 165.

protection, etc.'[118] The Court recognised 'informational privacy' as an important aspect of the right to privacy that can be claimed against state and non-state actors. The right to informational privacy allows an individual to protect information about herself and prevent it from being disseminated.[119] Further, the Court recognised that the right to privacy is not absolute and may be subject to reasonable restrictions. In order to limit discretion of State in such matters, the Court has laid down a test to limit the possibility of the State clamping down on the right – the action must be sanctioned by law, it must be necessary to fulfil a legitimate aim of the State, the extent of the State interference must be 'proportionate to the need for such interference', there must be procedural safeguards to prevent the State from abusing its power.[120] It has expressly recognised "protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits"[121] as certain legitimate aims of the State.

(ii) Legislative Developments

Though the *Puttaswamy* judgment is a landmark legal development in the discourse on privacy, especially informational privacy; prior legislative attempts have been made to secure informational privacy in various sectors in India. These includes the general data protection rules under the Information Technology Act, 2000 (IT Act) as well as various sector specific laws on data protection.

a. The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)

The SPDI Rules have been issued under Section 43A of the IT Act. Section 43A, relates to "Compensation for Failure to Protect Data" and enables the enactment of "reasonable security practices and procedures" for the protection of sensitive personal data. The SPDI Rules incorporate, to a limited extent, the OECD Guidelines, specifically: collection limitation, purpose specification, use limitation and individual participation.

The SPDI Rules mandate certain requirements for the collection of information,[122] and insist that it be done only for a lawful purpose connected with the function of the organisation.[123] In addition, every organisation is required to have a detailed privacy policy.[124] The SPDI Rules also set out instructions for the period of time information can be retained,[125] and gives individuals the right to correct their information.[126] Disclosure is not permitted without consent of the provider of the individual, or unless such disclosure is contractually permitted

[118] Per R.F. Nariman, J. at paragraph 42.
[119] Per D.Y. Chandrachud, J. at paragraph 142.
[120] Per S.K. Kaul, J., paragraph 71.
[121] Per D.Y. Chandrachud, at paragraph 185.
[122] Rule 5(1), SPDI Rules.
[123] Rule 5(2), SPDI Rules.
[124] Rule 4, SPDI Rules.
[125] Rule 5(4), SPDI Rules.
[126] Rule 5(6), SPDI Rules.

or necessary for legal compliance.[127] When it comes to sharing information with Government agencies, then the consent of the provider is not required and such information can be shared for purposes such as verification of identity, prevention, detection and investigation including of cyber incidents, prosecution, and punishment of offences.[128]

The SPDI Rules apply only to corporate entities[129] and leaves the government and government bodies outside its ambit; the rules are restricted to 'sensitive personal data', which includes attributes like sexual orientation, medical records and history, biometric information etc.,[130] and not to the larger category of personal data. Further, the Cyber Appellate Tribunal (CyAT) which hears appeals under the IT Act has issued its last order in 2011. The absence of an effective enforcement machinery therefore raises concerns about the implementation of the SPDI Rules. It is thus necessary to make a comprehensive law to adequately protect personal data in all its dimensions and to ensure an effective enforcement machinery for the same.

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

The Aadhaar Act enables the Government to collect identity information from citizens[131] including their biometrics, issue a unique identification number or an Aadhaar Number on the basis of such biometric information[132], and thereafter provide targeted delivery of subsidies, benefits and services to them.[133] The Aadhaar Act also provides for Aadhaar based authentication services wherein a requesting entity (government/public and private entities/agencies) can request the Unique Identification Authority of India (UIDAI) to verify/validate the correctness of the identity information submitted by individuals to be able to extend services to them.[134] The requesting entity is required to obtain the consent of the individual before obtaining her identity information for the purpose of authentication and must use her identity information only for the purpose of authentication.[135]

The Aadhaar Act establishes an authority, namely, the UIDAI, which is responsible for the administration of the said Act.[136] It also establishes a Central Identities Data Repository (CIDR)[137] which is a database holding Aadhaar Numbers and corresponding demographic and biometric information.[138] Under the Aadhaar Act, collection, storage and use of personal data is a precondition for the receipt of a subsidy, benefit or service.[139] Though the Aadhaar

[127] Rule 6, SPDI Rules.
[128] Rule 6(1), SPDI Rules.
[129] Section 43-A, IT Act.
[130] Rule 3, SPDI Rules.
[131] Section 30, Aadhaar Act.
[132] Section 3, Aadhaar Act.
[133] Section 7, Aadhaar Act.
[134] Section 8, Aadhaar Act.
[135] Section 8(2), Aadhaar Act.
[136] Section 11, Aadhaar Act.
[137] Section 10, Aadhaar Act.
[138] Section 2(h), Aadhaar Act.
[139] Section 7, Aadhaar Act.

Act does not *per se* make application for an Aadhaar Number mandatory (it is specifically provided as an 'entitlement' under Section 3) except for availing of certain benefits, subsidies and services funded from the Consolidated Fund of India, in practice, taking of Aadhaar Number is becoming mandatory for availing most services through a range of cognate laws.[140]

The Aadhaar Act and its regulations recognise various data protection principles, to ensure the security of information and privacy of Aadhaar Number holders. First, there is an obligation on the UIDAI to ensure security and confidentiality of the identity information and authentication records of individuals which includes taking all necessary steps to protect such information against unlawful access, use or disclosure, and accidental or intentional destruction, loss or damage.[141] Further, the Aadhaar Act prohibits the sharing of core biometric information, and the use of it for a purpose other than the generation of Aadhaar Numbers and authentication.[142] The sharing of information other than core biometric information is permissible under certain conditions. The Aadhaar Act also permits an individual to make a request to the UIDAI to provide her access to her identity information (excluding her core biometric information)[143] and her authentication records.[144] She can also seek rectification of her demographic data if it changes/is incorrect, and her biometric information if it is lost or changes.[145] Finally, the UIDAI will have no knowledge of the purpose of any authentication.[146]

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.[147]

Despite its attempt to incorporate various data protection principles, Aadhaar has come under considerable public criticism. First, though 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.[148] Concerns have also been raised *vis-a-vis* the provision on

[140] Komal Gupta and Suranjana Roy, 'Aadhaar to be mandatory for mobile phone verification', LiveMint (25 March 2017) available at http://www.livemint.com/Industry/wyGskI48Ak73ETJ5XW0diK/Aadhaar-now-a-must-for-all-mobile-phone-connections-after-ta.html (last accessed 5 November 2017); 'PTI, 'Linking Aadhaar number to bank accounts mandatory: RBI', Business Line, (21 October 2017), available at: http://www.thehindubusinessline.com/money-and-banking/linking-aadhaar-with-bank-account-is-mandatory-rbi/article9917776.ece (last accessed 5 November 2017).
[141] Section 28, Aadhaar Act.
[142] Section 29, Aadhaar Act.
[143] Section 28(5), Aadhaar Act.
[144] Section 32(2), Aadhaar Act.
[145] Section 31, Aadhaar Act.
[146] Section 32, Aadhaar Act.
[147] Regulation 3, Aadhaar Security Regulations.
[148] 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/ (last accessed 16 November 2017); Reetika Khera, 'No Good Will Come from Linking Aadhaar to Mid-Day Meals', The Wire (24 March 2017), available at https://thewire.in/118555/aadhaar-mid-day-meals/ (last accessed 16 November 2017).

Aadhaar based authentication which permits collection information about an individual every time an authentication request is made to the UIDAI.[149] Finally, despite an obligation to adopt adequate security safeguards, no database is 100% secure.[150] In light of this, the interplay between any proposed data protection framework and the existing Aadhaar framework will have to be analysed.

c. Financial Sector

Financial information, being a highly sensitive category of information, necessitates an adequate data protection regime for its protection. The primary legal instruments that address data protection in the financial sector include: the Credit Information Companies (Regulation) Act, 2005 (CIC Act), the Credit Information Companies Regulation, 2006 (CIC Regulations) and circulars issued by the Reserve Bank of India (RBI). Further, the SPDI Rules recognise financial information such as credit card, debit card and other payment instrument details as sensitive personal data, thus to that extent regulating their use, collection and disclosure.[151]

i. CIC Act

In the financial sector, provisions scattered across various statutes provide for an obligation to maintain customer confidentiality and adherence to data protection norms. However, the CIC Act, along with the CIC Regulations, is perhaps the legislation with the most comprehensive provisions on data protection in the financial sector.

The CIC Act primarily applies to credit information companies (CICs) and recognises them as collectors of information.[152] The CIC Act imposes an obligation on CICs to adhere to privacy principles at the stage of collection, use and disclosure of credit information[153], and requires them to ensure that credit information held by them is accurate, complete and protected against loss or unauthorised use, access and disclosure.[154] Similarly, the CIC Regulations impose an obligation on CICs to ensure data security and secrecy. It also requires them to adhere to a large number of recognised data protection principles such as: data collection limitation, data use limitation, data accuracy, data retention and access and modification.[155]

ii. RBI Circulars

[149] Jean Dreze, 'Hello Aadhaar, Goodbye Privacy', The Wire (24 March, 2017) available at https://thewire.in/118655/hello-aadhaar-goodbye-privacy/ (last accessed 5 November 2017)
[150] Subhashis Banerjee *et al.*, A Computer Science Perspective: Privacy and Security of Aadhaar, 52(37) Economic & Political Weekly (16 September 2017).
[151] Section 3(ii), SPDI Rules.
[152] Regulation 2(b), CIC Regulations.
[153] Section 20, CIC Act.
[154] Section 19, CIC Act.
[155] Chapter VI, Privacy Principles, CIC Regulations.

The Know Your Customer (KYC) norms limit the categories of information that banks and financial institutions can seek from their customers.[156] Once such information is collected, there is an obligation on banks to keep it confidential.[157] Further, multiple instruments such as the Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs,[158] the Master Circular on Customer Services, 2009[159] and the Code of Banks Commitment to Customers[160] etc. all provide for privacy and customer confidentiality obligations that have to be adhered to by various entities in the financial sector.

d. Telecom Sector

There are multiple laws that operate in the telecom sector such as the Indian Telegraph Act, 1885 (Telegraph Act), the Indian Wireless Telegraphy Act, 1933, the Telecom Regulatory Authority of India Act, 1997 (TRAI Act) and various regulations issued thereunder. However, data protection norms in the telecom sector are primarily dictated by the Unified License Agreement (ULA) issued to Telecom Service Providers (TSP) by the Department of Telecommunications (DoT).

The format in which, and the types of information that are to be collected from the individual is prescribed by the DoT.[161] A TSP has an obligation to take necessary steps to safeguard the privacy and confidentiality of the information of individuals to whom it provides a service and from whom it has acquired such information by the virtue of the service provided.[162]

Further, the TSP is obliged to maintain all commercial, call detail records, exchange detail records and IP detail records for at least one year for scrutiny by the DoT.[163]As far as security safeguards are concerned, there are multiple obligations prescribed for the TSP which includes inducting only those network elements into its telecom network which have been

[156] RBI Master Direction on Know Your Customer (KYC) Direction, 2016 dated 25 February 2016, updated as on 8 July 2016, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10292&Mode=0 (last accessed 13 November 2017). This Master Direction was amended by RBI Amendment to Master Direction dated 8 December 2016, available at https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=10770 (last accessed 13 November 2017).

[157] RBI Master Circular on Customer Service in UCBs dated 1 July 2015, available at: https://www.rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9863, (last accessed November 5, 2017).

[158] RBI Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Prepaid Card Operations of Banks and Credit Card issuing NBFCs, available at Master Circular on Credit Card, Debit Card and Rupee Denominated Cobranded Prepaid Card operations of banks dated 1 July 2014, available at: https://rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=8998 , (last accessed 5 November 2017). Some parts of this Circular were amended by RBI Notification on Customer Protection on Limiting Liability of Customers in Unauthorised Electronic Banking Transactions dated 6 July 2017, available at: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11040&Mode=0 (last accessed 13 November 2017).

[159] RBI Master Circular on Customer Service in Banks, 2015 dated 1 July 2015, available at: https://rbi.org.in/scripts/BS_ViewMasCirculardetails.aspx?id=9862 (last accessed 14 November 2017).

[160] Code of Bank's Commitment to Customers, 'Section 5- Privacy and Confidentiality', Banking Codes and Standards Board of India (June 2014), available at: https://www.dbs.com/in/iwov-resources/pdf/codeofbanks-aug091.pdf (last accessed 3 November 2017).

[161] Clause 39.17, Unified License Agreement.

[162] Clause 37.2, Unified License Agreement.

[163] Clause 39.20, Unified License Agreement.

tested as per the contemporary Indian or International Security Standards,[164] amongst others.[165] Finally, customer information can be disclosed only if the individual has consented to such disclosure and the disclosure is in accordance with the terms of consent.[166] In addition, the TSP has to make efforts to comply with the Telegraph Act which imposes an obligation on it to facilitate the Government to carry out 'interception' of messages in case of emergencies - a privacy intrusion justified largely in the name of national security. There are some procedural safeguards built into this process of interception.[167]

Further, the Telecom Regulatory Authority of India (TRAI) has framed the Telecom Commercial Communication Preference Regulations, 2010 (TRAI Regulations) to deal with unsolicited commercial communications.[168] The TRAI Regulations envisage the setting up of Customer Preference Registration Facility[169] by telecom service providers through which customers could choose to not receive commercial communications. However, these regulations are limited to messages and other communication through phones, and would would not cover an email application or advertisements appearing on browsers.

e. Health Sector

Despite the inherently sensitive nature of health information, the legal framework on data protection in the health sector appears to be inadequate. The Clinical Establishments (Central Government) Rules, 2012 (Clinical Establishments Rules) requires clinical establishments to maintain and provide Electronic Medical Records/Electronic Health Records, thus mandating the storage of health information in an electronic format.[170] The SPDI Rules recognise health information as constituting 'sensitive personal data' and thus regulates its collection, use and disclosure. However, as already mentioned the SPDI Rules apply only to the private sector thus leaving the whole of the public health sector outside its ambit.

The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (IMC Code) issued under the Indian Medical Council Act, 1956 mandate physician-patient confidentiality unless the disclosure of the patient's information is required by law, or if there is a serious and identified risk to an individual/community, or the disease is a notifiable one.[171] Interestingly, at the same time the IMC Code requires that the patient, her relatives and responsible friends have knowledge of the patient's condition so as to serve her best interests[172] thus allowing for disclosure without the consent of the patient. Further, physicians are encouraged to computerise medical records, maintain them for a period of three years and provide access to them to the patient upon her request.[173] However, the limited privacy

[164] Clause 39.7, Unified License Agreement.
[165] Clause 39, Unified License Agreement.
[166] Clause 37.2, Unified License Agreement.
[167] Rule 419-A, Telegraph Act.
[168] Regulation 2(i), TRAI Regulations.
[169] Regulation 3, TRAI Regulations.
[170] Rule 9(iv), Clinical Establishments Rules.
[171] Section 2.2., IMC Code.
[172] Section 2.3. IMC Code.
[173] Section 1.3.2, IMC Code.

safeguards and absence of an enforcement mechanism renders the IMC Code largely inadequate to address the concerns surrounding health information.

These existing laws and regulations will have to be analysed and changes, if any, concomitant with the introduction of a new data protection framework, suggested.

(iii) The AP Shah Committee Report

In 2012, a Group of Experts on Privacy was constituted by the erstwhile Planning Commisison under the Chairmanship of Justice AP Shah (Justice AP Shah Committee). The report of the Justice AP Shah Committee recommended a detailed framework that serves as the conceptual foundation for a privacy law in India, considering multiple dimensions of privacy. After a detailed deliberative and consultative exercise, it proposed a set of nine National Privacy Principles to be followed, broadly derived from the OECD Guidelines.[174] It also proposed a co-regulatory form of enforcement with privacy commissioners set up by statute along with self-regulatory organisations.[175] The principles recommended by the Justice AP Shah Committee as well as the model of enforcement deserve close scrutiny insofar as they relate to question of data protection.

5. Possible Approaches

As discussed above, the analysis of the data protection models followed by the EU and the US sets out two basic approaches: the EU model is a rights based one, where protection of personal data is equated with protecting the fundamental right to privacy. The EU model has been criticised however, for being excessively stringent, and imposing many obligations on the organisations processing data. At the other end of the spectrum is the US approach, which focuses on protecting the individual from excessive State regulation. The US model recognises the value of data *vis-a-vis* encouraging innovation, and therefore allows collection of personal information as long as the individual is informed of such collection and use. However it has been viewed as inadequate in key respects. Several hybrid models also exist. These approaches must be kept in mind alongside the recognition of the right to privacy by the Supreme Court of India and legislative and other developments which have already taken place in India.

At the same time, one must be mindful of the need to encourage innovation, recognised by the Supreme Court of India, in its decision holding privacy to be fundamental, yet limited by reasonable restrictions. In addition, India's potential to lead the world into a digital economy making use of its existing strengths in information technology, demographic dividend, and its need for empowerment based on data-driven access to services and benefits for the common

[174] The nine principles set out by the Justice AP Shah Committee are as follows:
Principle 1: Notice; Principle 2: Choice and Consent; Principle 3: Collection Limitation; Principle 4: Purpose Limitation; Principle 5: Access and Correction; Principle 6: Disclosure of Information; Principle 7: Security; Principle 8: Openness; Principle 9: Accountability
Report of the Justice AP Shah Committee, 21-27 (October 16, 2012).
[175] Report of the Justice AP Shah Committee, 5 (October 16, 2012).

man and woman must be kept in mind. Factoring in these diverse objectives, a nuanced approach towards data protection will have to be followed in India. It is to understand what these nuances are that this White Paper has been drafted for public consultation and comments.

This White Paper has been divided into three substantive parts:

Part II- Scope and Exemptions;
Part III- Grounds of Processing, Obligation on Entities and Individual Rights; and
Part IV- Regulation and Enforcement.

Each Part contains several Chapters comprising brief notes on every aspect that we envisage will form a part of a data protection law. Each note, in turn, sets out the key issues that need to be considered, international practices relevant in this regard, provisional views of the Committee based on its research and deliberations and questions for public consultation. For easy reference, a summary is provided at the end of the paper in Part V listing all questions for public consultation. The purpose of this exercise is to ascertain the views of key stakeholders and the general public on each of these aspects. It must be emphasised that this format for consultation has been followed based on the need to ensure targeted consultation with stakeholders. The provisional views of the Committee are meant to provoke discussion and debate and do not represent its final views in any manner. Further, the questions suggested for discussion are carefully formulated and would serve their purpose if careful and precise and answers are provided.