DATA PROTECTION – PROTECTION OF WHAT, PROTECTION FROM WHOM & PROTECTION FOR WHOM - AN ANALYSIS OF THE LEGAL AND JUDICIAL PROVISIONS IN INDIA AND ABROAD

*Shatakshi Singh**

Abstract

Governments around the world today find themselves shouldered with the dual responsibility of managing economies oiled by data and protecting individual privacy. Such a dichotomous situation begs clarity on three aspects of an effective data protection regime- protection of what, from whom and for whom. These three questions have today emerged as the most pensive issues regarding data protection that policymakers and interpreters around the world are faced with. The article seeks to answer these three questions drawing from the experiences of three parts of the world- the United States of America, the European Union and India. The article, after briefly introducing the concept and need of a data protection regime, discusses in some length the evolution of the right to privacy in India through an analysis of the judicial discourse on the same. Hereinafter, each of the three questions has been discussed in detail under three headers- each header

dealing with one of the three jurisdictions. Answers to the three questions, in context of the three countries under study, shed light on the three aspects of an effective data protection regime- personal data, data subject and data controller. The subsequent section builds upon the answers thus obtained to present a scheme of standards that have gained repute and accolade at the international level and use the same as a benchmark to critically analyse the current nuances of the data protection laws in India. The concluding section of the article indicates the need for a consolidated data protection regime in the country while discussing the recent developments towards the same which is taking shape in the form of the data protection bill.

I. INTRODUCTION AND OVERVIEW

A. The need to protect data- the beginning of a consciousness

With the advent of information technology and large-scale data transfer, there is a growing concern about the whereabouts and safety of personal data. The challenges that are faced with regard to protection and security of data have been recognized today on an international level.[1] From the early 1970s, a large amount of personal

*Shatakshi Singh is a fourth-year student at Symbiosis Law School, Noida. The author may be reached at shatakshisingh1996@gmail.com.

[1]*See* Organisation of Economic Cooperation and Development [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data*, C(80)58/FINAL (July 11 2013), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [hereinafter OECD Guidelines] ; G.A. Res. 217 (iii) A,

information was being processed with the use of computers.[2] This also was the time when the European Economic Community saw a boom in trans-border trade which led to sharing of personal information across borders. This burgeoning data synergy was greatly supported by the advent of the era of information technology.

At this point, it is imperative to understand the meaning of the term Data. The term is defined in section 2(o) of the Information Technology Act, 2000 as follows-[3]

> *"(o) 'data' means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized 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."*

The need to protect this data was not always felt in India. The realization that data can be construed as an asset linked to privacy that can ultimately be breached, mainly set in after the expansion of the trend of off- shoring business operations conducted in India.[4] However, when one talks about protecting data, one of the most important things is to ensure that the dual purpose of protection of

Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948); Council of Europe, Convention on the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14, Nov. 4, 1950, ETS No. 005 [hereinafter European Convention on Human Rights].

[2]Sian Rudgard, *Origins and Historical Context of Data Protection Laws*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, (Sept. 23, 1980), https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf.

[3]The Information Technology Act, 2000, § 2, No. 2, Acts of Parliament, 2000 (India).

[4]*See* Latha R. Nair, *Data Protection Efforts in India: Blind Leading the Blind*, 4 Indian J.L. & Tech. 19, 20 (2008).

privacy and free flow of data is achieved.[5] This kind of dual approach is quite evident in the European Data Protection Directive.[6]

In the Indian context, the framework for data protection is neither structured nor comprehensive. Rather, it is scattered across diverse legislations and constitutional decisions. However, much can be learnt about the data protection jurisprudence of the country by analysing the ultimate source of all data protection laws- the right to privacy. One of the earliest and most authoritative discourses on what constitutes 'right to privacy' can be obtained from the article written by Warren and Brandis in 1890.[7] The article pointed out that the common law, as was in existence then, was insufficient to protect individuals against breach of their privacy rights. They went on to assert that be it tort law, contract law or copyright laws, they all provide a limited and tailored protection against disclosure of personal data and that common law itself contained a more potent tool to protect the right- a tool that was yet to be interpreted. This tool was based on the right to be let alone. The right, as the authors argued was not a property right, rather it stemmed from the idea of "inviolate personality".

The discussion on privacy becomes important since right to privacy is the channel through which an individual can assert the right to control and monitor their personal information.[8] Hence, the right to protect personal information can be very well understood as a component of one's right to privacy. Apart from the statutory provisions, most of the judicial discourse available on data protection stem from one or the other interpretation of the right to privacy.[9] Not only the Indian

[5]*Id.*
[6]Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).
[7]Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).
[8]Glancy Dorothy, *Invention of the Right to Privacy*, 21 Ariz. L. Rev. 1, 40 (1979).
[9]*See infra*, note 18.

judiciary but courts in United States have also recognized the link between data protection laws and right to privacy.[10]

The international recognition of the link between the two kinds of rights is also evident from the European Union Charter of Fundamental Rights. Articles 7 and 8 of the charter talk about "respect for private and family life" and "protection of personal space".[11]

B. Development of Judicial Underpinnings of the Data Protection Discourse in India

The case of *Kharak Singh* v. *State of U.P.*[12] was one of the earliest decisions to deny the right to privacy the status of a fundamental right, though not in very clear terms. However, whether right to privacy can flow from the article 21 of the Constitution and be hence considered a fundamental right has long been a matter of debate owing to the different interpretations adopted by the Supreme Court in different cases.[13]

[10]*United States Dep't of Justice* v. *Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) (holding that one of the essential aspects of privacy is the ability to exercise control over one's personal information).

[11]Charter of Fundamental Rights of the European Union, Dec. 18, 2000, 2000 O.J. (C 364) 1.

[12]Kharak Singh v. State of U.P. 1963 AIR 1295 (holding that privacy is an essential ingredient of personal liberty under article 21 of the constitution of India).

[13]*See* Unni Krishna, I.P. & Ors. v. State of Andhra Pradesh (1993) AIR 2178; R. Rajagopal & Anr.v. State of Tamil Nadu and Ors. (1994) 6 SCC 632; Peoples Union of Civil Liberties (PUCL) v. Union of India & Anr. (1977) 1 SCC 301 (holding that the right to privacy flows directly from the right to right guaranteed under article 21 of the Indian Constitution). *See*, e.g., M.P. Sharma & Ors. v. Satish Chandra &Ors. AIR 1954 SC 300 (six judge bench held that right to privacy is not a guaranteed right under the constitution).

It has been pointed out by commentators[14] that the turning point in providing constitutional recognition to the right to privacy is the judgment of the Supreme Court in the case of *Gobind* v. *State of Madhya Pradesh*.[15] Though the court stayed shy of declaring right to privacy a fundamental right, it was nevertheless opined by the court that right to privacy found place in the penumbral zone associated with fundamental rights.

Justice Mathew explained the need of data privacy laws in a world where technology was taking personal data into uncharted territory.[16] In later judgments of the Supreme Court, though privacy was again not given an express status of a fundamental right, several components of privacy were sought to be given individual recognition. Hence, in *PUCL* v. *Union of India*,[17] Supreme Court held that unauthorized phone tapping abridged the right to privacy.

Then, in the year 2015 the Supreme Court of India, in the case of *K.S. Puttaswamy and Ors*. v. *Union of India and Ors*[18] held that the diverging opinions of the Supreme Court across different judgments on the right to privacy create a pertinent and pervasive question that must be answered by a nine-judge bench. On 24th February, 2017 the nine judge bench of the Supreme Court declared the right to privacy a fundamental right under article 21 of the constitution of India.[19] In doing so, the judgments in *M.P. Sharma* case and *Kharak Singh* case stand overruled.

[14]Lawrence Liang, *A Right for the Future*, The Hindu (Aug 29, 2017, 12:15 a.m.), http://www.thehindu.com/opinion/lead/a-right-for-the-future/article19576761.ece.
[15]Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
[16]*Id.* ("Time works changes and brings into existence new conditions. Subtler and far reaching means of invading privacy will make it possible to be heard in the street what is whispered in the closet").
[17]PUCL v. Union of India (1996) 2 SCC 752 (holding that right to privacy could not be considered a fundamental right).
[18]K.S. Puttaswamy and Ors. v. Union of India and Ors (2015) 8 SCC 632.
[19]K.S. Puttaswamy and Ors. v. Union of India and Ors (2017) SCC OnLine SC 996.

C. Impact of the Puttaswamy Judgment (2017) On Data Protection in India

By giving the right to privacy a constitutional status, the judgment has laid down the constitutional edifice for a data protection regime.[20] Justice Chandrachur has pointed out the need to balance the protection of sensitive personal data against national security.[21] The judgment lays down some broad rubrics for the data protection regime without actually directing the legislature to frame rules for the same. The judgment will also have a far reaching consequences on the fate of the challenge to the Aadhar Act before a five judge bench of the Supreme Court.[22] Clearly, the judgment will provide impetus to the legislature to pass a comprehensive law on the subject of data protection thereby bringing the data protection regime in India, in line with that of Europe and U.S.A.

The *Puttuswamy* judgement, in more ways than one has transformed the way in which a common man views the right to privacy. By making informational privacy a part of the broader right to privacy,[23] the judgement has provided a jurisprudential backing to the coveted data protection regime that has oft been ignored while interpreting the constitutional right to privacy.[24] The judgement has laid the foundation on which the legislature, by means of a data protection act, can legitimately indulge in a balancing act between the interests of the individual and needs of the state with respect to protection of personal

[20]Agnidipto Tarafder And Arindrajit Basu, *For the Many and the Few: What a Fundamental Right to Privacy Means for India*, The Wire (Aug 25, 2017, 12:00 a.m.), https://thewire.in/170988/right-to-privacy-supreme-court-2/.
[21]Puttuswamy, *supra* note 18 at ¶ 179.
[22]*Id.*
[23]*Id.* at ¶ 177.
[24]Live Law Staff, *This Is What Supreme Court Said In Right To Privacy Judgment*, Live Law (Aug 24, 2017, 12:00 a.m.), http://www.livelaw.in/supreme-court-said-right-privacy-judgment-read-judgment/.

information. The concluding section of the paper will build upon the discourse that has been created by the judgement.

II. PROTECTION OF WHAT

In this nascent stage of information technology, data protection laws have been hailed as a novel area of law.[25] As has been already specified in the beginning of this paper, 'data' in the present study refers to personal data. However, the ambit of personal data is not easy to define. It can assume different forms in different places over different periods of time. Hence, it is important to understand what exactly data protection laws across the globe seek to protect.

Labelled as the "currency" of digital economy, protection of personal data has assumed great importance in this electronically interconnected globalised world.[26] Across most of the definitions of personal data, it is recognised that personal data has the capability to 'identify' an individual.[27] If personal data can be considered the currency of the digital economy then big data can be definitely referred to as a jackpot.[28] In the simplest terms big data is an uncontrolled explosion of digital data- a kind of situation where the 'management' of the bulk of data becomes impossible because of lack

[25]Stephanie J. Frazee, *Bloggers as reporters: An Effect Based Approach to First Amendment protections in a New Age of Information Dissemination*, 8 Vand. J. Ent. & Tech. L. 609, 640 (2006).
[26]Diane A. MacDonald, Christine M. Streatfield, *Personal Data Privacy And The WTO*, 36 Hous. J. Int'l L. 625, 626 (2014).
[27]*Id.*
[28]JAMES MANYIKA ET AL., *BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY, (*McKinsey Global Inst. ed.,2011) (Defining Big Data as data bases that are too mammoth in size to be handled by typical database software tools to manage, analyse capture and store).

of tools to 'measure' it[29].Many have pointed out that big data leads to development of transformative innovation. However, the downside of the story reveals the potent threat that personal data can pose when stored and transmitted around the world in the form of big data.

It should be further noted that personal data can refer to personal as well as commercial aspects of information. Though both fall within the ambit of personal data, they produce different results when breached. Protection of personal aspects of information falls within ambit of privacy rights while protection of commercial aspects falls in the realm of proprietary rights. Hence, data protection entails both privacy as well as proprietary rights.

Given the different interpretations that can be accorded to the term personal data, it is important to understand the scope and ambit of the term across various legislations around the world.

A. Position in the U.S.A

The U.S.A. has a sectoral data protection law. This is because the laws are fragmented and spread across governmental and industry specific regulations. The U.S.A does not recognize a fundamental right to privacy.[30] Nor does the constitution in the U.S.A accord direct protection to the right to privacy. Nevertheless, the right can be implicitly derived from the First, Third, Fourth, Fifth, and Fourteenth amendment.[31]

[29]Andrew McAfee, Erik Brynjolfsson, *Big Data: The Management Revolution*, Harvard Business Review (Oct, 2012), https://hbr.org/2012/10/big-data-the-management-revolution.

[30]*See* Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I- The Current Impact of Surveillance on Privacy*, 66 Colum. L. Rev. 1003, 1032 (1966) (noting that the right to privacy can be compromised on the altar of general public welfare).

[31]*See* U.S. Const. amends. I, III, IV, V, XIV; Griswold v. Connecticut, 381 U.S. 479, 483-85 (1965); Roe v. Wade, 410 U.S. 113, 153 (1973).

To address the question of what U.S.A.'s data protection laws protect, it is observed that the industries which contain data protection laws are those which handle or transmit sensitive personal information. Before discussing in detail the ambit of personal data it is imperative to first list some of the most important Federal laws on Data protection that exist in the U.S.-

- Federal Trade Commission Act-[32] it is a consumer protection law that seeks to curb the deceptive trade practices and has been also extended to the offline and online privacy and data security policies. The companies that fail to comply with posted privacy policies face enforcement actions under the act for the disclosure of personal data.[33]

- The Financial Services Modernisation Act-[34] it regulates the use, disclosure and collection of financial information.[35]

- The Health Insurance Portability and Accountability Act ["HIPAA"]-[36] it is a provision to regulate the medical information and can apply to data processors, health care providers, pharmacies and other entities.[37]

- The Electronic Communications Privacy[38] Act and The Computer Fraud and Abuse Act[39]- while the former

[32]Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1914).
[33]Leuan Jolly, *Data Protection in The United States: Overview*, Thomson Reuters (Jul 1, 2017), https://uk.practicallaw.thomsonreuters.com/6-502 467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.
[34]Financial Services Modernisation Act, 15 U.S.C §§ 6801- 6827 (1999).
[35]*Supra* note 21.
[36]The Health Insurance Portability and Accountability Act, 42 U.S.C et sq. (1996).
[37]*Supra* note 21.
[38]Electronic Communications Privacy, 18 U.S.C § 2510 (1986).
[39]The Computer Fraud and Abuse Act, 18 U.S.C §1030 (1984).

> protects the interception of electronic communication, the latter regulates the tampering of computer resources.

Apart from the above federal laws, there exist several state laws as well that protect personal data. California is the leader in this field and has enacted several personal data privacy laws whose importance resonates even at the national level.[40]

Now it is essential to come to the main question in discussion under this section- i.e. "What data is regulated?" Much like the nature of the data protection laws available across the United States, the answer to this question is also scattered and fragmented and depends on the law under consideration. For example, the FTC Act does not explicitly mention the category of data that it seeks to protect. What it prohibits are such practices that can potentially render the personal information of consumers at the risk of exploitation and hacking.[41] Such personal information would include consumers' searches online, the web pages visited, the contents viewed etc.

The FSM Act regulates the personal information that is collected from consumers who avail financial services and products for commercial or non- commercial purposes from a financial institution.[42] Hence, the personal information here mainly refers to the financial personal information of the consumer.

[40]The law in California mandates a state body or a business entity to send due notice to any resident of California in case his/her unencrypted personal information has been acquired or is reasonably believed to have been acquired, *see* California Civ. Code, § 1798.29(a)(1977) (for state bodies); California Civ. Code, § 1798.82(A) (1977) (for businesses).

[41]Federal Trade Commission Act, 15 U.S.C. § 45b(b)2 (1914).

[42]*See* Financial Services Modernisation Act, 15 U.S.C § 6802 (1999).

Similarly, within the purview of HIPAA, personal information would mean individually identifiable health and medical information.[43]

Again, as per California Security Breach Notification Law, any individual's first name or first initials and last name together with social security no., Driver's License, Account No., Credit or debit Card No, Medical Information or Health Insurance Information would constitute personal information.[44] Hence, it can be seen that the thrust is on that combination of information that can potently identify an individual.

It has been noted that in the United States, the definition of "personal information" remains uncertain.[45] While certain legislations like the Electronic Communication Privacy Act[46] seek to protect the personal information of individuals in transitory, final or stored communication (wire, oral and electronic communication), others like the Computer Fraud and Abuse Act[47] protect a wide variety of personal information including defence related information, financial transaction data etc. In fact, legislations like the Children's Online Privacy Protection act[48] and Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records[49] employ particularly circular definitions of personal data. While the former defines personal data as the data which provides individually identifiable information about an individual, the latter defines personal data as that data which identifies an individual. Clearly this

[43]The Health Insurance Portability and Accountability Act, 42 U.S.A §1301 et sq. (1996).
[44]*Supra* note 40.
[45]*See* McKay Cunningham, *Complying With International Data Protection Law*, 84 U. Cin. L. Rev. 421, 425 (2016)
[46]Electronic Communication Privacy Act, 18 U.S.C. § 2510-22 (1986).
[47]Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986).
[48]Children's Online Privacy Protection Act, 15 U.S.C § 6501(8).
[49]Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records, 18 U.S.C § 2725 (2000).

lack of consistency has led to widespread regulatory uncertainty and discord.

B. Position in the E.U.

Privacy has been declared a fundamental right in the E.U.[50] Unlike the sectoral approach to Data Protection legislation adopted in the U.S.A, the E.U., for the purpose of regulating the use and transfer of personal data, enacted a common legislation.[51] Under this legislation the term personal data has been defined as follows-

> *"Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular byreference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."*[52]

The above definition is wider than the U.S definitions. Under the EU legislation whenever someone links a certain piece of information to a specific person, that information will be considered personal, even if the link is not apparent to the person holding the information. [53] This can be understood in light of the fact that even IP addresses and cookies have been recognised as personal data by The Working Party on Data Privacy.[54] Some entities try to evade the data privacy laws by

[50]*See* Pamela Samuelason, Privacy as Intellectual Property?, 52 STAN. L. REV. 1125, 1134 (2000).
[51]Council Directive 95/46/EC, *supra* note 6, arts. 5-6 [henceforth EU Directive].
[52]*Id*. art. 2(a).
[53]*See* OAUL m. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U.L. Rev. 1814, 1819 (2011).
[54]Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search engines*, E.U., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

making the information anonymous.[55] Since such data cannot be identified with any particular individual the attempt is to take it effectively outside the ambit of personal data. However, it has been recently brought to light that even anonymous data can reveal information through carefully coded algorithmic scripts.[56]

Hence, the EU Directives'[57] definition of what is personal data is far more ambitious and multifaceted than the definitions prevalent in the U.S.A. The consolidated nature of the law in form of the directive[58] gives coherence and structure to the ambit of Personal Data and hence facilitates efficient implementation of Data Protection norms. This efficiency arises from the lack of ambiguity about whether a certain piece of information would qualify as 'personal' or not. The directive, by including data which indirectly identifies an individual within the ambit of personal data, has accorded greater protection to the identity of an individual. Here, it is imperative to mention that on 25 May, 2016 the EU General Data Protection Regulations[59] were adopted after a number of deliberations. By 25 May, 2018 the new regulations shall replace the current Directive (EU 95/46/EC). In broad terms, the GDPR defines personal Data as any information that can be directly or indirectly used to identify a natural person. It can include anything from the email address, bank details till the photo of the individual.[60]

[55]*See* Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harv. J. Of Law and Tech 1 (2011).
[56]Arvind Narayan, Vitaly Shmatikov, *Myths and Fallacies of 'Personally Identifiable Information'*, Communications Of The Acm, (Jan 27, 2011), https://cacm.acm.org/.../2010/...myths-and-fallacies-of-personally-identifiable-inform.
[57]EU Directive.
[58]*Id.*
[59]Council Regulation 2016/679 of Apr. 27 2017 on The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter EU GDPR].
[60]Sivarama Krishna et al., *Demystifying the EU General Data Protection Regulation*, PwC, (Sept, 2016), http://www.pwc.in/assets/pdfs/consulting/cyber-security/demystifying-the-eu-general-data-protection-regulation.pdf.

It is to be noted here that unlike the old directive, where the member states of EU were required to come up with their own legislations on data protection (within the wide ambit of the directive), the new GDPR seeks to create uniformity in the substantive part of the data protection regulation.[61] It envisages a transfer of power in the hands of the individual to exercise control over the processing of their personal data.[62] By including 'biometric' and 'genetic information' within the ambit of personal data, the GDPR will go a long way in ensuring that every aspect of personal information is protected.[63]

C. Position in India

India neither has consolidated data protection laws such as the EU, nor does it have sectoral laws such as exist in the U.S.A. However, this does not imply an absolute absence of legal protection in this regard. As already discussed, there exists in India, a rich stock of judicial decisions on the right to privacy which have been construed as giving way to the right to protection of personal data. Other than such jurisprudence, data protections norms can be culled out from The Indian Contract Act, 1872,[64] The Information Technology Act, 2000,[65] The Information technology (Amendment) Act 2008 and the 2011 rules implementing some of the provisions of the IT amendment act, 2008.[66] Other than the above provisions, the use of financial information is regulated by The Credit Information Companies

[61]However, some room will be provided for the individual states to legislate on the procedural aspects of the legislation, *see* Aditi Chaturvedi, *Comparison of General Data Protection Regulation and Data Protection Directive*,The Centre For Internet & Society (Feb 7, 2017), https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive.
[62]*Id.*
[63]*Id.*
[64]The Indian Contract Act, 1860, No. 9, Acts of Parliament, 1872 (India).
[65]*Supra* note 3.
[66]Notification no. G.S.R. 313(E), April 11, 2011, Extraordinary, Part 2, § 3(i), Gazette of India.

(Regulation) Act, 2005[67] and to a certain extent by The Prevention of Money Laundering Act, 2002.[68]

As per the 2011 rules, personal information has been defined as information which in combination with some other information available or likely to be available with a body corporate relates to the identity of an individual either directly or indirectly.[69] The rules however mark a separate category or subset of personal information in the form of Sensitive Personal Information.[70] Any personal information that relates to the following is termed as sensitive data-

a) Passwords
b) Financial information
c) Physical, psychological and mental health condition
d) Sexual orientation
e) Medical records and history
f) Biometric information
g) Any information from (a)-(f) received by a body corporate for provision of services; or
h) Any information relating to (a)-(g) that is received, stored or processed by the body corporate under a lawful contract or otherwise.

It is to be further noted that information available under the Right to Information Act 2005[71] is exempt from the above two definitions.[72] Certain other classes of information like religious beliefs, ethnicity and political opinions are also not covered under definition of

[67]The Credit Information Companies (Regulation) Act, No. 30, Acts of Parliament, 2005, (India).
[68]The Prevention of Money Laundering Act, No. 15, Acts of Parliament, 2003, (India).
[69]*Id*. at Rule 2(i)
[70]*Id*. at Rule 3.
[71]Right to Information Act, No. 22, Acts of Parliament 2005 (India).
[72]*Id.*

sensitive information. Such information does find mention in the sensitive personal information category in other jurisdictions either.[73]

Under the CIC Act, personal information entails all the information that needs to be necessarily furnished by the customer to establish his/her identity.[74] The CIC regime accordingly mandates the CICs, Credit Institutions and the others to establish concrete principles for the collection and use of such personal information.

Here it is to be noted that the draft Personal Data protection Bill 2006 introduced in Parliament on 18th October 2010 lapsed without being realised into a law.[75] Further in 2011 and 2014 a non-profit organization called Centre for Internet and Society released draft privacy Bills on the Internet that recognized individual's right to privacy but allowed invasion of the same for some larger considerations.[76] Further, in May 2016 it was asserted by the Minister for Communication and Information Technology Mr. Ravishankar Prasad that the government was still working on the proposed law.[77] It should be noted that the draft of the proposed privacy bill defines personal data as[78] data which relates to a living, natural person if that person can be identified from that data in conjunction with other data the controller has or is likely to have.

[73]Sreenidhi Srinivasan, Namrata Mukherjee, *Building an Effective Data Protection Regime*, Vidhi Centre For Legal Policy (Jan, 2017), http://vidhilegalpolicy.in/public-law/.
[74]The Credit Information Companies (Regulation) Act, §§ 14 & 17, No. 30, Acts of Parliament, 2005, (India).
[75]Raghunath Ananthapur, *India's new Data Protection Legislation*, 8 SCRIPTED 192, 2013 (2011).
[76]Aditi Subramaniam, *The Privacy, Data Protection and Cybersecurity Law Review*, The Law Review (Nov, 2016), http://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-3/1140175/india.
[77]*Id.*
[78]Hari Subramaniam, Data Protection 2017, ICLG, (May 15, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/india.

Further, the sensitive personal information has been defined by the bill as relating to unique identifiers such as-[79]

a) Aadhar number or PAN;
b) Physical and mental health;
c) Biometric or genetic information
d) Banking credit and financial data; and
e) Narco Analysis and /or Polygraph test data.

Hence, it is clear that legislation in India is diverse on the issue of ambit of personal data. A comparison between the three countries reveals that India needs to adopt a broad umbrella legislation with an expansive definition of 'personal data' on the lines of the EU laws. The EU directive states that all data with which an individual can be identified or is identifiable, should fall within the ambit of personal data. Following from this, the definition of personal data in India must not be myopic so as to be limited only to that information which directly relates to an individual. Since the IT Act and Rules prescribe the ambit of personal data in the form of pointers referring to a certain type of personal information, it should be replaced with a more general approach like that of EU wherein any information is construed as personal information if it either directly or indirectly leads to the identity of an individual.

Also, unlike in the U.S.A, India should not experiment with sectoral definitions of personal data. A scattered definition would add to the entropy that already exists in India due to the absence of a comprehensive data protection regime.

[79] *Id.*

III. PROTECTION FROM WHOM

The next question to be addressed is against whom should such protection be sought. In modern democracies, there has been an upsurge in cross border data trade. With data being collected and transferred not just by the government but also, at a faster pace, by the private sector.[80]

With respect to the government, its desire to accumulate more and more personal data about its subjects has grown over the past decade. This increase in appetite for personal data of individuals stems from a new model of administration that governments across the globe seem to have adopted- 'data processing model of administrative control'.[81] Personal data is being collected for a variety of purposes like taxation, issuance of license, voter registration, employee identity verification, law enforcement etc. The new threats to national security in the form of terrorist attacks has added further impetus for the government to seek personal data of every individual who goes in and out of the country.[82] It is to be noted however, that though the need/desire on part of government to collect personal information has existed for a long time, the accessibility to the same has considerably increased over the past decade.[83] This has mainly happened due to two reasons-

The *first* relates to the sharp increase in the amount of data being generated and transmitted from within the country to other countries. Hence, information related people's lives in the industrialised world is increasingly available in other countries. The *second* reason stems

[80]Shrishti Saxena, *Data Protection in India*, LIVE LAW (May 15, 2017), http://www.livelaw.in/data-protection-india/.
[81]Paul Schwartz, *Data Processing and the Government Administration*: *The Failure of the American Legal Response to the Computer*, 43 Hatings Law J., 1321, 1326 (1992).
[82]*Id.*
[83]*Id.*

from the fact that government can today easily access personal data of its subjects from third party sources.[84]

Considering these factors, the attempt will now be to analyse the situation in the United States, the E.U., and India to determine against which entity the data protection laws of these jurisdictions seek to accord protection. The answer to this question will in a large way affect the future of data privacy across a world where the demarcation between public and private is fast waning.

A. Position in the U.S.

As already discussed, the data protections laws in the U.S.A are highly sectoral and unlike the E.U. there is no comprehensive legislation on the same. This peculiar nature of the data protection laws makes it difficult to clearly pinpoint the exact authorities against which the laws seek to accord protection. However, it can be generally stated that the federal laws seek to regularize the collection and dissemination of personal data by "consumer reporting agencies",[85] oversee the collection and handling of personal data by federal governmental agencies,[86] and mandate financial service corporations to adopt such measures as would ensure the privacy and safety of consumer's personal data. [87] Hence, despite being very diversified, the data protection laws are pitched to provide protection against both the public and the private sector.

However, it is essential to understand that the data protection jurisprudence that developed in the U.S. was the result of inherent and

[84]Fred H. Cate, James X. Dempsey, and Ira S. Rubinstein, *Systematic Government Access to Private Sector*, International Data Privacy Law (Sept. 17, 2012), https://oup.silverchair-cdn.com/oup/backfile/Content_public/Journal/idpl/2/4/10.1093/idpl/ips027/2/ips027.pdf.
[85]Fair Credit Reporting Act, 15 U.S.C. § 1681 (West 2014).
[86]Privacy Act of 1974, U.S.C. § 552a (West 2014).
[87]Gramm- Leach Bliley Act, 15 U.S.C. §§ 6801- 6809 (West 2011).

inborn suspicion in the minds of the citizens regarding the misuse of state power.[88] This can be seen in light of the fact that modern laws on data protection can trace their origin to the Bill of Rights which sought to impose restrictions on State power.[89] In modern times, in fact, the data protection laws stem from the recognition that was accorded to privacy by US Courts under the Fourth Amendment.[90]

Apart from the data protection legislations that accord protection to the American citizenry against both private and governmental encroachment on personal data, a rich judicial discourse further strengthens this protection against the government and it agencies, through a string of case laws. In one of the much-acclaimed articles by Samuel Warren and Louis Brandeis it has been asserted that the best way to protect personal data is by keeping it outside the public domain.[91]

Though protection to personal data has been provided against both the government and the private sector, the multitude of the legislations has left much task of interpretation in the hands of the judiciary. Hence a trend has emerged to the effect that in most of the complaints regarding data breaches, either against the government or the private

[88]*See* James Q. Whitman, *The Two Western Cultures of Privacy: Digital Versus Liberty*, 113 Yale L.J. 1151, 1153 (2004).
[89]*Id.* at 1211-12.
[90]*See* City of Ontario v. Quon, 560 U.S. 746, 755-56 (2010) (Holding that the Fourth Amendment guarantees that the invasive and encroaching acts of officers of government does not evade privacy, dignity and security if citizens); Olmstead v. United States, 277 U.S. 438,478 (1928) (Holding that the citizen in the U.S. had the right of be left alone against the government and that the framers of the U.S. constitution had sought to protect the citizens in their beliefs, thoughts, emotions and sensations).
[91]Samuel Warren, Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1980).

sector, the judiciary demarcates the limits of data protection on a case to case basis.[92]

B. Position in Europe

Europe, unlike U.S.A has a very comprehensive and well defined system of data protection laws that recognises right to privacy as a fundamental right.[93] Considering the technological boom in the 1960s, and the rapid use of computers for storing citizens' personal data *en masse*, a need was felt to accord protection against both private entities and the government.[94] Accordingly, the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data was presented by the Council of Europe for adoption by the European Nations. It came to be known as Convention 108 and is the only legally binding instrument that exists in the area of Data Protection. [95]The most striking feature of the Convention is that it equally applies to public and private entities as long as they are involved in collecting personal data.[96]

Following this, on October 24, 1995 Directive 95/46/EC was issued by the Council of Europe and the European Parliament on the "Protection of Individuals with regard to the processing of personal data and on the free movement of such data." [97] Even though the members of EU have already integrated the principles of Convention 108 in their national laws, a need was felt to have a comprehensive

[92]Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 Penn. St L. Rev. 587, 600 (2007).
[93]Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14 art. 8(1), Nov 4, 1950, ETS No. 5.
[94]Christina Glon, *Data Protection in The European Union: Closer Look at the Current Patchwork of Data protection Laws and the Proposed Reforms That Could Replace Them All*, 42 Int'l J. Legal Info. 471, 492 (2014).
[95]COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW (2014).
[96]*Id.*at 62.
[97]*Id*. at 6.

law that would give common cross border definitions of the various aspects of data protection laws.[98]

Another contribution made by the Directive was that it clearly demarcated the ambit of the term controller and processor of personal Data. Under the EU laws a controller is a person who –

> *"Alone or jointly with others determines the purpose and means of the processing of personal data".* [99]

Any entity that can be held responsible under the applicable law and falls within the ambit of the definition of Data Controller shall be considered the same. This means that any natural or legal person in the private sector and any authority in the public sector can be held responsible as a data controller.[100] From here it can be fairly concluded that the Directive applies equally to the private as well as the public sector.

Such a comprehensive coverage ensures a wholesome protection to the personal data of the data subjects such, without any bias towards either the public or the private sector.

Further, in December 2000, The European Council and the European Parliament together passed Regulation (EC) No. 45/2001.[101] This regulation has expanded the scope of Directive 95/45/EC to all 'community institutions and bodies" other than governmental bodies. A European Data Protection Supervisor has been appointed as an independent supervisory entity to ensure proper enforcement of the

[98] *Id.* at 62.
[99] Data Protection Directive, art. 2(d).
[100] *Id*. at 64.
[101] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on The Protection of Individuals With Regard to The Processing of Personal Data by The Community Institutions and Bodies on The Free Movement of Such Data, 2001 O.J. (L 8)1, 3 [hereinafter Regulation (EC) 45/2001].

regulation. This further ensures that a large gamete of public authorities is brought within the ambit of Data Protection laws.

Under the newly formulated EU GDPR,[102] any organization involved in the processing (which included collection and dissemination) of personal data can be divided into two categories- data controller and data processor. The organization that collects personal data from the consumers is called the data controller. The controller has the power to ascertain the manner in which this personal information is to be used.[103] This data controller can further send the personal data to other entities for processing purposes. Hence organizations that are involved in mere storage and processing of the personal data on behalf of the controller are called data processors.[104] Both of these entities would be under the scrutiny of the EU GDPR.

C. Position in India

Despite the lack of a comprehensive framework, there are certain legislations that cover the aspect of data protection and provide some relief, howsoever limited, in the area. Apart from these legislations, the courts in India have played an active role in developing the culture of data protection by giving an expansive definition to the Right to Privacy.

When it comes to statutory provisions, the most important and comprehensive one on the issue of data protection is the Information and Technology Act, 2000, amended by the Information Technology Amendment Act (2008).[105] This act provides for civil prosecution[106] in the case of "Cyber contraventions" and criminal action[107] in the

[102]EU GDPR.
[103]*Supra* note 39.
[104]*Id.*
[105]The Information Technology Act, 2000, No. 2, § 2, Acts of Parliament, 2000 (India).
[106]*Id.* at § 43(a)-(h).
[107]*Id.* at §§ 63-74.

case of "cyber offences". The main question under this section, however, is to understand the entities against which the laws in India seek to accord protection. The IT Act as amended in 2008 provides 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 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."*[108]

Hence the act provides protection to sensitive personal data against body corporate, i.e., companies, sole proprietorships or associations that collect or process sensitive personal data.[109] It is to be noted that the provision nowhere mentions any public authority and refers to only corporate entities. Even if one were to resort to section 72A one would find that it protects the contractual obligation between a company and its customer in relation to disclosure of sensitive personal information. However, it is to be noted that unlike section 72 of the IT Act 2000 which was limited to authorities and service providers, section 72 A provides protection against any person who handles personal data under the terms of a lawful contract. However, neither of the above sections provide any effective protection of data against government entities.[110] The fact that public authorities are excluded from the ambit of the major provisions relating to data protection, seriously limits the scope of the law. Even the IT Rules of

[108]*Id.* at §43 A.
[109]Asang Wankhede, *Data Protection in India and the EU: Insights in Recent Trends and Issues in the Protection of Personal Data*, 2 Eur. Data Prot. L. Rev. 70, 79 (2016).
[110]*Id.*

2011 provide extensive rules for data protection only against the corporate entities.[111]

On an analysis of the above jurisdictions and on the basis of discussion in an earlier section, it can be fairly concluded that just like the U.S., the Indian judiciary has played an important role in evolving the data protection jurisprudence. The U.S. however, protects the privacy right of individuals through judicial discourse as well as legislation- wherein the legislation accords protection against the private entities as well as the state. In India on the other hand, the entire legal framework provides protection only against the activities of private bodies. The judiciary, through expansive interpretations of the right to privacy has indeed heralded a new chapter in data protection against the government, but much needs to be done in terms of legislation to bring government and related entities within the ambit of privacy laws. Like the U.S the EU also accords protection against both the public as well as private sector but unlike the U.S the EU provides this wholesome protection under an umbrella law. Hence it can be seen that just like the previous section on 'protection of what', it can be fairly concluded that India needs a unified data protection regime which accords protection against the private sector as well as government entities.

IV. PROTECTION FOR WHOM

The concern over the protection of personal information has become a widespread phenomenon across the globe. People today, more than

[111]Hari Subramaniam, Aditi Subramaniam, *Data protection 2017*, ICLG, (15 May, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/india.

ever before are concerned about the threats posed to data privacy from the public as well as the private sector.[112]

Across all the geographical areas in consideration, i.e., U.S, E.U. and India, the cynosure of the provisions relating to data protection is the individual. Per the E.U. Data Protection Directive[113] Data Subject is –

> *"Any identifiable or identified natural person- meaning thereby who can be identified directly or indirectly.*[114]

In fact, some countries have left the definition of "data subject" totally outside the purview of any statute. An example on point is the U.S. wherein none of the statutes define the "data subject".[115]

Coming to the Indian context, it has been pointed out, that with reference to the IT Rules 2011[116], the distinction between "the provider of information" and the person "to whom the data pertains" i.e. the Data Subject can cause lot of confusion in terms of defining the rights of the individual whose identity can potentially be disclosed by the personal information.[117]

---

[112]David Banisar, Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Development*, 18 J. Marshall J. Computer & Info. L. 1, 3 (1999).

[113]Council Directive 95/46, 1995 O.J. (L281) 31 (EC) ch 1 art. 2(a).

[114]Donald C. Doling, Jr., *International Data Protection Law*, White & Case, (Aug, 2009), https://intellicentrics.ca/wp-content/uploads/dlm_uploads/2014/09/article_intldataprotectionandprivacylaw_v5-1.pdf.

[115]Aaron P. Simpson, Jenna Rode, *Data Protection- 2017 (U.S.A)*, ICLG, (May 15, 2017), https://iclg.com/practice-areas/data-protection/data-protection-2017/usa.

[116]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R 313(E), Gazette of India, section 3(i)(India).

[117]Radha Raghavan, Ramya Ramchandran, *Data Protection Law in India: An Overview*, LEX- WARRIER, (Jan 29, 2013), http://lex-warrier.in/2013/01/indias-data-protection-law-an-overview/.

V. THE INTERNATIONAL BENCHMARK AND INDIA

After having undertaken a comprehensive analysis of the major components of the data protection laws across three different geographical regions, this section seeks to shed some light on the tenets of Indian Data protection laws (particularly the IT Act, 2008 and the IT Rules 2011) and their international credibility. It is to be noted that the major aspects of the IT Act and the Rules in terms of Data subject, Data Controller and the nature of data have already been discussed in the previous sections. This section aims to elucidate upon the technical aspects of data processing that the law envisages.

India, being one of the most popular outsourcing destinations, witnesses the inflow and outflow of a huge quantity of data across its borders.[118] This large data market requires robust regulatory measures and the same will be discussed in the present section. However, before moving to the Indian scenario it is important to briefly understand the international standards that are expected out of a data protection regime.

A. The International Benchmark for Data Protection

There is no authoritative compilation stating the exact standards that a data protection law is expected to follow. However, there are certain works of authority which give a general idea of the horizons of data protection laws through a set of principles. It is noted by Bennet and Raab that a set of twelve "fair information principles" have been widely acknowledged as covering the major dimensions of fair data protection laws.[119]

[118]Probir Roy Chowdhury, Soumya Patnaik, *Data Protection in India*, TAYLOR WESSING (May, 2015), https://www.taylorwessing.com/globaldatahub/article_dp_cyber_india.html.
[119]Graham Leaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, 23 J.L. Inf. & Sci. 4, 9 (2014).

These principles are- accountability; collection with knowledge; use limited to identified purpose; retention only as long as required; individual correction; data kept accurate; limited collection to where necessary for purpose; purpose identification; security safeguards; openness on policies and practices; individual access and data quality.[120] Hence any data protection regulation should be an international embodiment of these twelve principles tailored as per the national needs.[121]

Other than the above set of principles, several other sets of data protection bench marks are also available.[122] Apart from these, there are certain other international instruments which throw light on the facets of data protection laws.[123] Two of these are the OECD privacy Guidelines of 1981[124] and the Council of Europe (CoE) Data Protection Convention 108 of 1981.[125] If the standards laid down in these two instruments are combined, a comprehensive set of principles concerning data protection can be obtained. The principles can be summarized as follows[126]

Collection of data

- *Data Quality*
- *Collection*
- *Purpose Specification*

[120]*Id.*
[121]*Id.*
[122]Some authors have also included 'sensitivity' amongst the important principles that a data protection law is expected to follow, *see* e.g., LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 11-12 (BOOK ED. 2002).
[123]European Convention on Human Rights ETS 5, (Nov. 3, 1950) art. 8(1) (1950).
[124]OECD Guidelines.
[125]ETS No. 108, *supra* note 72.
[126]*See supra* note 98.

Communication to data subject

- *Uses & disclosures limited to purpose specified or compatible*
- *Openness in personal data practices*
- *Mandatory data sharing*

Notice of purpose and rights at the time of collection

- *Individual's right to access data*
- *Individual's right to correct data*

Security Measures

- *Security through reasonable safeguards.*
- *Accountability of data controller.*

Having stated the basic principles that data protection laws across the world are expected to follow, it is now essential to analyse in some detail the adherence of the provisions relating to data protection in India, to these standards.

B. Analysing the Data Protection Regime in India

The embodiment of the international standards in data protection laws can be best found in the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (IT Rules).[127]

These rules have attempted to introduce several of the above principles, like purpose specification, consent, collection, limitation etc., in the Indian data protection regime. Section 43A of the IT act[128]

[127]Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R 313(E), Gazette of India, section 3(i)(India) (hereinafter IT Rules).
[128] The Information Technology Act, 2000, No. 2, § 43A, Acts of Parliament, 2000 (India) (hereinafter IT Act).

which uses the words 'sensitive personal information' and 'reasonable security practices', reserves the scope of making rules for defining the same.[129]

The scope of the section 43A and the IT Rules have already been discussed in previous sections, however, it is essential here to reiterate that the provisions apply only to 'body corporates' that handle 'personal information' or 'sensitive personal information'.[130] The definition of body corporate as given in section 43A totally excludes government entities and individuals from its purview.

Following are some of the major provisions of the Rules which can be analysed in terms of adherence to the international standards laid down for data protection laws-

a) Consent to the collection of information

To understand the requirement of consent in the collection of information, it will be helpful to peruse into the bare provision which is as follows-

> *"Rule 5. Collection of information- (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information."*[131]

It is to be noted that both the individual and a third party can be the source of personal information about the individual. Rule 5(3) of the IT Rules specify that when the source of collection of personal information is the individual (whose personal information is being

[129]Srinivasan, *supra* note 48.
[130]IT Act, § 43A.
[131]Rule 5(1), IT Rules.

collected) himself, the details of the intended recipients, purpose of collection, contact details of collecting and storing entities etc. should be made known to him.[132]

In cases where the personal information about a person is being obtained from a third party source, all the accompanying rights such as right of access etc., will be available to the third party and not to the data subject. This provision clearly dilutes the requirement of consent of the person to whom the personal data actually pertains.[133]

Moreover, an organization that has collected the personal information cannot disclose the same without the prior permission of the information provider.[134] However, if such disclosure was already permitted in the original contract between data provider and receiver then there is no requirement of prior consent. It is to be noted here that this provision is a variation of the internationally acceptable 'use limitation' principle of data protection laws. [135]

b) Communication of Information to Data Subjects

The important component of this rule lies in the mandatory privacy policy that all organisations dealing with personal information are supposed to have in place. The organizations are further required to make this privacy policy available in public domain so that the providers of information can readily view it. The organizations are expected to publish information about the purpose and usage of data collected, types of data collected, and the reasonable security practices that have been adopted by the organization, etc.[136] This principle is drawn from the 'openness' or 'notice' principle of data

[132]Rule 5(3), IT Rules.
[133]The person to whom the personal data directly pertains is often refered to as the 'Data Subject'; Srinivasan, *supra* note 48.
[134]Rule 6, IT Rules.
[135]OECD GUIDELINES.
[136]Rule 4, IT Rules.

privacy acceptable at the international level.[137] However, the mere fact that an organization has in place an internally developed privacy policy does not absolve it from the other norms that are to be followed under an effective data protection regime.[138]

Apart from the requirement of disclosing the privacy policy, there also exists a notice requirement. Notice pertaining to certain important details like intended recipients, contact details of collecting and storing organizations need to be made known to an individual when data is being collected directly from him.[139] However this information does not include within its ambit, details regarding right to limit use and disclosure, or right to ask for erasure of certain pieces of information.[140] This limits the individual's capability to exercise control over personal data.

c) Mandatory Data Sharing

Whenever sharing of information with the government is mandated under any law, the organizations do not need any consent from the data subjects or the data providers before disclosing personal or even sensitive personal information pertaining to them.[141] The rationale is that the government will always use personal data of people for purposes of maintaining law and order. Such personal information can aid the government to detect, prevent and investigate instances of cyber-crime. However, there is one minor safeguard provided. The government will have to send the request for seeking the personal information in writing to the organization and will have to also specify the purpose of seeking information relating to that particular

[137]*Supra* note 113.
[138]PLANNING COMMISSION OF INDIA, *REPORT OF GROUP OF EXPERTS ON PRIVACY*, (CHAIRED BY JUSTICE A.P SHAH), (2012).
[139]Rule 5(3), IT Rules.
[140]*Id.*
[141]Proviso to Rule 6(1), IT Rules.

individual or group of individuals.[142] The government is also supposed to state that the information so obtained will not be shared with any other person.[143] However, there is no limitation on the period for which the government can hold such information.[144] Also, even after the investigation using the information obtained has come to an end, there is no provision to let the data subject know that personal information relating to him was shared in the first place. The fact that section 43A is entirely focused on the body corporate, again excludes any protection against the government matters of data protection. [145]

d) Right to Access Information

The rules provide that the provider of information (the data subject or the third person provider of information), has the right to review information pertaining to them and ask for corrections in case there are any irregularities.[146] The rules further provide that every organization is supposed to designate one grievance officer who is to take complaints from the providers of information in respect of any discrepancy in information pertaining to them.[147] Such an interface will greatly facilitate increased control of the provider of information on their personal data. Also, the fact that the rules mandate the resolution of the disputes within a month puts the Indian data protection regime a step forward in achieving international standards.[148]

Though the above provision is a positive step towards empowering the data provider (and not necessarily the data subject), it is to be

[142] *Id.*
[143] *Id.*
[144] REPORT OF GROUP OF EXPERTS, *Supra* note 126.
[145] Srinivasan, *supra* note 48.
[146] Rule 5(6), IT Rules.
[147] Rule 5(9), IT Rules.
[148] Rule 5(9), IT Rules.

noted that currently the organization collecting and storing personal data is under no obligation to notify a data subject in the case of breach or change in privacy policy.[149] Another drawback of the rules is that while the information providers have the right to withdraw consent given earlier,[150] there are no guidelines laid down to indicate the course to be followed by the organization (that collects personal information), once the consent has been withdrawn.

e) Security Measures

The practices that aim to protect information from unauthorized access, disclosures etc., are designated as 'reasonable security practices' under section 43A of the IT Act.[151] The practices are supposed to be prescribed by agreement or law and in absence of the same they need to be prescribed by the central government. The security policies that are required to be put in place should cover technical, organizational and physical security measures. They are also required to follow some prescribed international security standards.[152] Such compliance will again ensure that the data protection regime that organizations are envisaging can match up to the international standards.

[149]Report of Group of Experts, *supra* note 116.
[150]Rule 3(7), IT Rules.
[151]Explanation (ii), § 43A, IT Act.
[152]The International Standard IS/ISO/IEC 27001 on "*Information Technology – Security Techniques - Information Security Management System – Requirements*" is specified to be one such security standard, Srinivasan, *supra* note 48.

VI. CONCLUDING REMARKS: PITCHING TOWARDS A CONSOLIDATED DATA PROTECTION REGIME IN INDIA

"India has a unique opportunity to draft a very modern data protection and privacy Bill which can be superior to what is happening elsewhere in the world."

- Nandan Nilekani[153]

In 2012 the AP Shah Report suggested the setting up of a consolidated legal data protection regime in India on the lines of the practices followed across the world.[154] Transparency, consent and accountability were identified as the fundamental building blocks of the regime.[155] These suggestions, however, were never implemented in the form of a law. A bill was introduced as a private members bill in parliament in 2009 by Baijayant "Jay" Panda titled "The Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill". It had the basic aim of protecting customers from unwarranted telephone calls from business promoters.[156] Other than the above, several other private members bills were also introduced on the subject that could never transform into a law.[157]

[153]Kunal Talgeri, *India Needs a Security and Privacy Law: Nandan Nilekani, Former Chairman*, UIDAI, ECONOMIC TIMES (Apr 29, 2017, 10:31 a.m.), http://economictimes.indiatimes.com/opinion/interviews/india-needs-a-security-and-privacy-law-nandan-nilekani-chairman-former-uidai/articleshow/58424580.cms.

[154]Supratim Chakravorty, Soumyadri Chattopadhyay, *Imagining India's New Data Privacy Law*, BUSINESS LINE (Aug 17, 2017), https://www.khaitanco.com/PublicationsDocs/HinduBusinessLine-KCOCoverage17Aug17Supra.pdf.

[155]*Id.*

[156]Kazim Rizvi, *High Time India has a Right to Privacy Law*, LIVEMINT (Jul 30, 2017, 7:14 p.m.), http://www.livemint.com/Opinion/EcRER0qfjd1ooT1twFzdVJ/High-time-India-had-a-right-to-privacy-law.html.

[157]Rajeev Chandrashekhar, Vivek Gupta and Om Prakash Yadav in the years 2010, 2016 and 2016 introduced private members bill on the citizens right to privacy, *Id.*

Recently, the Unique Identification Authority of India informed a nine- judge bench of the Supreme Court that the centre had constituted a committee led by former Supreme Court judge B.N. Srikrishna to demarcate "key data protection issues" and on the basis of the same, suggest a draft data protection bill.[158] The committee was constituted on 31st July 2017. The ministry of Electronics and Information Technology will aid the panel to chalk out a data protection regime that is tailored per the Indian needs. The aim of the government is to come up with a bill that is similar to the "technology neutral" draft Privacy Bill prepared by the erstwhile Justice A.P. Shah Committee and submitted to the Planning Commission. At that point of time, no positive actions were taken in regard to the A.P. Shah committee.[159] It is to be noted that M.P. Baijayant "Jay" Panda again tabled a private members Data (Privacy and Protection) Bill, 2017 in the Lok Sabha under which he proposed that right to privacy be given the status of a fundamental right.[160] The bill also aims to differentiate between data collector and processor. The A.P. Shah committee draft bill further states that in the case of a data breach, it would be the responsibility of the intermediaries to inform the individual within a definite period of time.[161]

In the *Puttuswamy* judgement, the Supreme Court made overt recommendation to the centre to come up with a "data protection regime".[162] Accordingly, the Government of India set up a committee of experts under former Supreme Court judge B.N Srikrishna to make

[158]Krishna Rajagopal, *Privacy Argument Will Hit Governance*, The Hindu (Aug 2, 2017, 12:43 a.m.), http://www.thehindu.com/news/national/centre-constitutes-new-panel-under-former-sc-judge-to-prepare-draft-data-protection-law/article19402660.ece.

[159]*Id.*

[160]*Id.*

[161] Kazim, *supra* note 138.

[162]Puttuswamy, *supra* note 18 (holding that the "regime" would require a careful balance between the privacy interest of the individual and the larger concerns of the state).

policy suggestions on data protection and draft a bill on the same. Accordingly, the committee published the white paper on 27 November, 2017 in which it has made exhaustive recommendations, the scope and ambit of which, will be discussed in the present section.

A. An Analysis Of The Draft Bill Suggested By Srikrishna Committee

Before going into the contents of the white paper, some insight into the discussions of the committee members while working on the white paper, will be most resourceful. In response to an RTI filed by Mr. Paras Nath Singh, the committee revealed the minutes of its meeting dated 8thSeptmber, 2017 and 3rd October, 2017.[163]

The minutes reveal that Justice B.N. Krishna increasingly emphasised on the data protection regime being in the form of an umbrella law that will deal with varied facets.[164] The kind of regulatory framework that the committee envisages for India can be culled out from the four working groups that the committee has formed, namely-[165]

1. Working group on Big Data Ecosystem and other emerging technologies – which will deal with the technical aspects of the regime and analyse the pros and cons of data collection, and processing.
2. Working group on Scope and Exemption of Law- which will deal with issues of applicability of data protection laws. Applicability includes territorial limits, exemption from application etc.

[163]Apoorva Mandhani, *Justice B.N. Srikrishna Committee Discloses Minutes Of Meetings; Reveals Circulation Of Draft Data Protection Bill By MeiTY*, LIVE LAW (Feb. 12, 2018), http://www.livelaw.in/justice-b-n-srikrishna-committee-discloses-minutes-meetings-reveals-circulation-draft-data-protection-bill-meity/.
[164]*Id.*
[165]*Id.*

3. Working group on grounds of processing and rights and obligations of parties- which will deal with the core legal issues associated with the control and transfer of personal data collected.
4. Working group on enforcement- which will deal with timely and flawless enforcement of the laws.

From the above listing of the working groups it is clear that the committee is pitching for a structured and responsive regime that can embrace the enormity of the subject that it seeks to control, i.e., data. A perusal into the white paper would reveal that the committee is keen to adopt and implement international standards with adequate tweaks to keep it in sync with Indian best practises.[166]

As per the committee, an ideal data protection regime should be based on seven principles- namely, flexibility of law, applicability of law to both public and private sector, consent must be meaningful, informed and genuine, there should be minimal data processing, strict accountability of those responsible for data processing, creation of a data protection statutory authority and lastly, imposition of adequate penalties for any violation.[167]

To analyse the provisions of the committee better, it is imperative to do so in context of the three questions that form the premise of this study.

[166]Committee Of Experts (Headed By Justice B.N. Srikrishna), White Paper On A Data Protection Framework For India (2017) (hereinafter Srikrishna Report).
[167]Vatsav Khullar, *Report Summary-White Paper on Data Protection Framework for India*, PRS Legislative Research, (Dec 1, 2017), http://www.prsindia.org/administrator/uploads/general/1514525011~~Report%20Summary%20-%20Data%20Protection%20Expert%20Committee%20White%20Paper.pdf.

A. Protection of What-

The Report recognises that the aim of a data protection regime should be to uphold the autonomy of the individual. This autonomy can be protected by guarding the personal data related to the individual. Hence, the personal data should be such that a particular individual is the cynosure of the data. In other words, the data should be about the individual.[168] However, all information related to an individual would not come within the ambit of personal data, i.e., only the data that can potentially lead to the 'identity' of an individual would qualify.[169] Further, the report categorises health information, genetic information, information related to religious beliefs and affiliations, sexual orientation and information related to racial and ethnic origin as sensitive personal data that ought to be accorded a higher pedestal of secrecy and protection.[170]

B. Protection from Whom-

The report, in very clear terms, states that a huge chunk of personal data is being processed in both the public as well as private sector.[171] Noting that in jurisdictions like EU, the data protection laws apply to both the public as well as privates sector, the report calls for a similar regulatory framework for India as well.[172] Hence, as the report points out, the need is to come up with a data protection law that encompasses both the public as well as private sector. Almost in the same breath, the report also treads a cautious path by suggesting that certain

[168] *See supra* note 179, at 46.
[169] The report states as an example that though a car registration number would not directly reveal the identity of an individual it can possibly reveal the identity of the same individual when clubbed with other relevant information. Hence, the registration no. should qualify as personal data, *see Id.*
[170] *Id.* at 61.
[171] *Id.* at 12.
[172] *Id.* at 41.

public entities can be reasonably exempted from the rigours of the law.[173]

C. Protection to whom-

The report at every point seeks to grant protection to the individual. Noting that by 2020, global volume of digitally created data will reach 44 zettabytes, of which a large chunk will be data related to individuals, the report seeks to protect individuals' interest and uphold their right to privacy as recognised in the *Puttuswamy* judgement.[174]

B. The Road Ahead- Recommendations for a draft Data Protection Bill

The Srikrishna committee has adopted a consultative process to fathom the Indian opinion on the ideal data protection regime. Making recommendations on a proposed legislation of such length and breadth would require an effective balance of the interests of all the stakeholders involved. Here, the author attempts to address some key concerns that data protection regime in India ought to follow.

The proposed recommendations can be best understood under the following two headers-

a) <u>The Content of the Regime</u>

[173]Noting however, that it is highly doubtful if total exemption should be provide to any government entity from data protection laws. Also, borrowing from the Puttuswamy judgment, the report points out that for the well-defined categories of the departments of government and similar entities in the private sector, reasonable exemptions may be made.

[174]*Id*. at 11.

An ideal data protection regime in India should have immense clarity. Most of the legislations in India till date have only evasively discussed the definition and ambit of the key terms associated with data protection.[175]

The new data protection regime should include clear definitions of personal and sensitive personal information wherein the scope of the former should be wide enough to embrace all data through which an individual can be identified or is identifiable.

Further, given the millennial fears of the government slowly metamorphosing into a surveillance state, the law should accord protection not just against the private sector but also the government and other public bodies.

Also, both the data processor (the one who uses the data for a purpose) and the data controller (one who has general supervision over the data but doesn't necessarily use/process it) should be brought within the ambit of the law.

Emphasis should also be paid on the following aspects-[176]

1. The discourse on consent-

The consent should be explicit and unambiguous. For example, suppose a woman X works for a company. The company has all the details of the women including her mail-id. There are certain specific uses that her email can be put to about which X has notice. However, if the company were to enter into a contract with another company for

[175]As noted earlier, the IT Act 2008 as well as the IT Rules, 2011 accord protection only against "body corporate" and "persons who handle personal information under terms of a contract". None of them deal with the responsibility of the government for an alleged personal data breach. Further, the ambit of sensitive personal information under IT Rules, 2011 does not include information pertaining to race, religion, ethnicity etc.

[176]Parag Mathur, *What The Upcoming Data Protection Law Means*, LIVEMINT (Jan. 17, 2018), http://www.livemint.com/Money/qYWLeoRFYj8gjS2v3LEIzK/What-the-upcoming-data-protection-law-means.html.

sharing employee information that the latter plans to use for an employee survey, an explicit consent of X should be taken.

Further, the degree of consent should vary according to the type of personal information that is sought to be collected.

2. The amount and extent of data that should be sought-

The data controller should seek only that much data that is adequate for the purpose for which it is sought. This is the test of 'minimum necessary data required for a particular purpose'.

3. Techniques of enforcement-

The minimum standards that are expected out of a data controller/processor should be implemented in the form of 'best practises certifications'. Under this policy certificates of healthy data protection practises should be provided to public and private entities that deal with personal data.

4. Scope to erase personal data once shared-

An individual should have the right to, subject to some restrictions, exercise discretion with regard to the time period for which his/her personal data is available with the data subject. A right to be forgotten from the digital space is essential in a democratic country.

b) <u>The Structure of the Regime-</u>

1. Whether a single law should govern both the public and the private sector-

The *Puttuswamy* judgement recognised right to privacy as a fundamental right 'enforceable against the state'.[177] This judicial discourse however, leaves a pertinent question unanswered- what about the horizontal application of the right to privacy with respect to the private bodies? There is no clarity at present whether right to privacy can be enforced against private citizens

[177]Puttuswamy, *supra* note 18.

or not.[178] However, there can be no ambiguity in the assertion that when the enforcement mechanisms against the private and government bodies are different, there is no need for the same regulation to govern both of them.

Also, given the potentially coercive power of the state to extract information from the citizens (as contrasted form the more voluntarily nature of disclosure in the case of private bodies), a more robust regulatory mechanism should be devised to tame governmental manoeuvres in collecting personal data of citizens.

2. The Powers of the Data Protection Authority-

A perusal into the Srikrishna committee shows that it envisages a powerful authority that wields wide and punitive powers. The authority will presumably act in close cohesion with the government. If the authority gets the power to sieve through the data of private firms under the pretext of data audits, firms might spiral down into the realms of redtapism.[179]

It also needs to be noted that unlike jurisdictions like EU, India has often seen wide powers vesting in the hands of few (across the public or private sector). Clearly, under such circumstances, a centralised authority for data protection can have serious consequences for freedom of expression as well as freedom of economic competition. Hence, separate Data Protection Authorities should be made to regulate the public and the private sector.

[178]Prashant Reddy, *One Data Protection Law and Regulator to Rule Them All?*, THE WIRE (Dec, 2017), https://thewire.in/202497/data-protection-law-regulator-india/.

[179]The author takes the example of social networking sights to point out that all pervasive control of a regulatory authority over these social networking sites, might trample the ease with which views and opinions are shared on them. Under the guise of protecting the personal data of the individuals, the authority might assume control over the discretion of the individual regarding the type of information he/she wants to share. *Id.*

It is expected that in light of the positive developments in the international arena towards a comprehensive and uniform data protection regime, India will take effective steps towards materializing a comprehensive legal data protection framework. In developing a consolidated law on data protection, it is imperative that the government ensures the active involvement of all the stake holders, especially the data subject. Such a wholesome framework will channelize the big data revolution towards increased prosperity of the nation and its individuals.