A Free and Fair Digital Economy

Protecting Privacy, Empowering Indians

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna

TABLE OF CONTENTS

GLOSSARY OF TERMS

S. No.	Defined Term	Definition
1.	Aadhaar Act	The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
2.	AI	Artificial Intelligence
3.	ALRC	Australian Law Reform Commission
4.	ALRC Report	For Your Information: Australian Privacy Law and Practice (Australian Law Reform Commission Report 108).
5.	CAG	Comptroller and Auditor General of India
6.	CCI	Competition Commission of India
7.	CLOUD Act	The Clarifying Lawful Overseas Use of Data Act, 2018 (US)
8.	Committee	Committee of Experts on a Data Protection Framework for India under the chairmanship of (retd.) Justice B.N. Srikrishna
9.	Competition Act	Competition Act, 2002
10.	Contract Act	The Indian Contract Act, 1872
11.	COPPA	Children's Online Privacy Protection Act, 1998 (US)
12.	CRC	United Nations Convention on the Rights of the Child
13.	CrPC	Code of Criminal Procedure, 1973
14.	CVC	Central Vigilance Commission
15.	Cyber Security Law of China	People's Republic of China Cyber Security Law of 2016
16.	Data Protection Directive of 1995	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
17.	DPIA	Data Protection Impact Assessment
18.	DPO	Data Protection Officer
19.	DPA	Data Protection Authority
20.	EEA	European Economic Area
21.	EU	European Union
22.	EU GDPR	European Union General Data Protection Regulation
23.	FIPP	Fair Information Practice Principles
24.	FISA	Foreign Intelligence Surveillance Act, 1978 (US)
25.	FISC	Foreign Intelligence Surveillance Court
26.	FTC	Federal Trade Commission
27.	GDP	Gross Domestic Product
28.	GLB Act	Gramm Leach Bliley Act (US)

29.	Income Tax Act	Income Tax Act, 1961
30.	Investigatory Powers Act, 2016	Investigatory Powers Act (UK)
31.	IRDA Act	Insurance and Regulatory Authority of India Act, 1999
32.	IT Act	Information Technology Act, 2000
33.	MLAT	Mutual Legal Assistance Treaty
34.	NATGRID	National Intelligence Grid
35.	NETRA	Network Traffic Analysis
36.	NIA Act	National Investigation Agency Act, 2008
37.	OECD	Organisation for Economic Cooperation and Development
38.	PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, 2001 (US)
39.	PMLA	Prevention of Money Laundering Act, 2002
40.	POPI Act	Protection of Personal Information Act, 2013 (South Africa)
41.	RBI	Reserve Bank of India
42.	RTI Act	Right to Information Act, 2005
43.	SEBI	Securities and Exchange Board of India
44.	SEBI Act	Securities and Exchange Board of India Act, 1992
45.	SPD Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
46.	Telegraph Act	The Indian Telegraph Act, 1885
47.	Telegraph Rules	Indian Telegraph Rules, 1951
48.	TOR	Terms of Reference of the Committee
49.	TRAI	Telecom Regulatory Authority of India
50.	TRAI Act	Telecom Regulatory Authority of India Act, 1997
51.	UK	United Kingdom
52.	UK DPA	The Data Protection Act, 1998
53.	UK Data Protection Bill	Data Protection Bill [HL] 2017-19
54.	US	United States of America

CHAPTER 1: A FREE AND FAIR DIGITAL ECONOMY

This report is based on the fundamental belief shared by the entire Committee that if India is to shape the global digital landscape in the 21st century, it must formulate a legal framework relating to personal data that can work as a template for the developing world. Implicit in such a belief is the recognition that the protection of personal data holds the key to empowerment, progress, and innovation. Equally implicit is the need to devise a legal framework relating to personal data not only for India, but for Indians.

Such a framework must understand from the ground up the particular concerns and aspirations pertaining to personal data shared by Indians, their fears and hopes. It is a platitude that such viewpoints may not necessarily be the same in developed countries, which already have established legal frameworks. The report thus ploughs its own furrow, responding to the challenges that India faces as a developing nation in the Global South. At the same time, it adopts learnings from best practices that exist in developed democracies with considerably advanced thinking on the subject.

A. Existing Approaches to Data Protection

In today's world, broadly three approaches to data protection exist. The US follows a *laissez-faire* approach and does not have an overarching data protection framework. 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.[1] Consequently, certain legislation, the Privacy Act, 1974, the Electronic Communications Privacy Act, 1986 and the Right to Financial Privacy Act, 1978 protect citizens against the federal government. With regard to the private sector, while no omnibus legislation exists, it has sector-specific laws that have carefully tailored rules for specific types of personal data. For example, the GLB Act[2] has well-defined provisions for collection and use of financial data.[3]

The EU, at the vanguard of global data protection norms has recently enacted the EU GDPR, which has come into force on 25 May 2018. This replaces the Data Protection Directive of 1995. It is a comprehensive legal framework that deals with all kinds of processing of personal data while delineating rights and obligations of parties in detail. It is both technology and sector-agnostic and lays down the fundamental norms to protect the privacy of Europeans, in all its facets. We are informed that 67 out of 120 countries outside Europe largely adopt this framework or that of its predecessor.[4]

[1] Roe v. Wade 410 U.S. 113 (1973); 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, 37 Texas Tech Law Review (2005).

[2] The GLB Act is also known as The Financial Services Modernization Act of 1999.

[3] A noted data protection scholar, Graham Greenleaf has argued in his submission that the US approach cannot be called a 'model' since no other country follows it. See comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee at p. 4.

[4] Comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee at p. 4.

Though the aforementioned approaches have dominated global thinking on the subject, recently, China has articulated its own views in this regard. It has approached the issue of data protection primarily from the perspective of averting national security risks. Its cybersecurity law, which came into effect in 2017,[5] contains top-level principles for handling personal data. A follow-up standard (akin to a regulation) issued earlier this year adopts a consent-based framework with strict controls on cross-border sharing of personal data.[6] It remains to be seen how such a standard will be implemented.

Each of these regimes is founded on each jurisdiction's own understanding of the relationship between the citizen and the state in general, and the function of the data protection law, in particular.[7] In the US, the *laissez-faire* approach to regulating data handling by private entities while imposing stringent obligations on the state is based on its constitutional understanding of liberty as freedom from state control.[8] Data protection is thus an obligation primarily on the state and certain categories of data handlers who process data that are considered worthy of public law protection. In Europe on the other hand, data protection norms are founded on the need to uphold individual dignity.[9] Central to dignity is the privacy of the individual by which the individual herself determines how her personal data is to be collected, shared or used with anyone, public or private. The state is viewed as having a responsibility to protect such individual interest. China, on the other hand, frames its law with the interests of the collective as the focus, based on its own privileging of the collective over the individual.

B. Understanding the Contours of the Indian Approach

Each of these legal regimes described above has acceptability in its respective jurisdiction because it captures the zeitgeist of the citizen-state relationship that exists in each. At the

[5] Cyber Security Law of China.

[6] Standard number: GB/T 35273-2017 available at <http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4FFAA51D63BA21B9EE40C51DD3CC40BE> (last accessed on 20 April 2018).
Further, see Samm Sacks, New China Data Privacy Standard Looks More Far-reaching than EU GDPR, Centre for Strategic and International Studies (2018) available at <https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr> (last accessed on 20 April 2018).

[7] For an insightful account on cultural bases for privacy protections, see James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty, 113 Yale Law Journal 1151 (2004).

[8] This derives from the American Declaration of Independence, 1776 a charter of limited government.
"We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, That whenever any Form of Government becomes destructives of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organising its powers in such forms, as to them shall seem most likely to affect their Safety and Happiness."

[9] This is succinctly stated in the Census Act Judgment of the German Constitutional Court on 15 December, 1983 recognising a right to informational self-determination.
"From this follows that free development of personality presupposes, in the context of modern data processing, protection of individuals against the unrestricted collection, storage, use and transfer of their personal data. This protection is therefore subsumed under the fundamental right contained in Article 2.1 in conjunction with Article 1.1 of the Basic Law ("human dignity shall be inviolable")."
Unofficial translation available at <https://freiheitsfoo.de/census-act/> (last accessed on 9 May 2018).

same time, it is trite that neither is India's understanding of its citizen-state relationship, nor its motivations for a data protection law, exactly coincident with each of the aforementioned jurisdictions. The conceptualisation of the state in the Constitution is based on two planks — first, the state is a facilitator of human progress. Consequently, it is commanded by the Constitution in Part IV (Directive Principles of State Policy) to serve the common good;[10] second, the state is prone to excess. Hence it is checked by effectuating both a vertical (federal structure) and horizontal (three organs of government) separation of powers, as well as by investing every individual with fundamental rights that can be enforced against the state.

The right to privacy has been recently recognised as a fundamental right emerging primarily from Article 21 of the Constitution, in *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*.[11] To make this right meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good. It is this understanding of the state's duty that the Committee must work with while creating a data protection framework.

The TORs (annexed in **Annexure A**) mandate both a study of various data protection related issues in India along with specific suggestions for a data protection framework and a draft bill. This must be seen in light of the objective of the Government of India in setting up of the Committee, also contained in the TORs, "to unlock the data economy, while keeping data of citizens secure and protected." This objective appears to be based on the salient realisation that data has the potential to both empower as well as to harm.

The transformative potential of the digital economy to improve lives in India and elsewhere, is seemingly limitless at this time. Artificial Intelligence holds out the promise of new breakthroughs in medical research[12] and Big Data generates more calibrated searches and allows quicker detection of crime.[13] Large-scale data analytics allows machines to discern patterns and constantly improves services in an endless virtual loop. The prospects of such data gathering and analysis to benefit citizens is immense.

---

[10] Specifically, Article 39(b) and (c) of the Constitution direct the state to make policy towards securing distributed ownership and control of material resources and preventing concentration of wealth to common detriment.

[11] 2017 (10) SCALE 1.

[12] The use of AI in the health industry in India is well documented. For instance, in the context of hospitals the Manipal Hospital Group has partnered with IBM's Watson for Oncology for the diagnosis and treatment of seven types of cancer, while in the context of pharmaceuticals, AI software is being used for scanning through all available academic literature for tasks such as molecule discovery. For further details and more instances of the use of AI in healthcare see E. Hickok et al, Artificial Intelligence in the Healthcare Industry in India, The Centre for Internet and Society, India (undated) available at <https://cis-india.org/internet-governance/files/ai-and-healtchare-report> (last accessed on 19 April 2018).

[13] For predictive policing, see Rohan George, Predictive Policing: What is it, How it works, and its Legal Implications, The Centre for Internet and Society, India (24 November 2015) available at <https://cis-india.org/internet-governance/blog/predictive-policing-what-is-it-how-it-works-and-it-legal-implications> (last accessed on 20 April 2018); For details on the potential of data analytics for the detection of money laundering see, Business Today (12 October 2016) available at <https://www.businesstoday.in/current/economy-politics/how-big-data-and-analytics-can-help-india-fight-against-money-laundering/story/238397.html> (last accessed on 19 April 2018).

At the same time, the potential for discrimination, exclusion and harm is equally likely in a digital economy. The recent admission by Facebook that the data of 87 million users, including 5 lakh Indian users, was shared with Cambridge Analytica through a third-party application that extracted personal data of Facebook users who had downloaded the application as well as their friends, is demonstrative of several such harms - users did not have effective control over data. Further, they had little knowledge that their activity on Facebook would be shared with third parties for targeted advertisements around the US elections. The incident, unfortunately is neither singular, nor exceptional. Data gathering practices are usually opaque, mired in complex privacy forms that are unintelligible, thus leading to practices that users have little control over. Inadequate information on data flows and consequent spam or worse still, more tangible harms,[14] are an unfortunate reality. Equally, the state collects and processes significant amounts of personal data of citizens, with much of such processing being related to its functions. Despite the fact that the State is able to exercise substantial coercive power, and despite ambiguous claims to personal data that may not be necessary for its functions, the State remains largely unregulated on this account.

Currently, the law does little to protect individuals against such harms in India. The transfer of personal data (defined as "sensitive personal data or information") is governed by the SPD Rules.

The SPD Rules were issued under Section 43A of the IT Act which holds a body corporate liable for compensation for any negligence in implementing and maintaining reasonable security practices and procedures while dealing with sensitive personal data or information. The SPD Rules expand on the scope of these reasonable practices and procedures. They define sensitive personal data[15] and mandate the implementation of a policy for dealing with such data.[16] Further, various conditions such as consent requirement,[17] lawful purpose,[18] purpose limitation,[19] subsequent withdrawal of consent,[20] etc., have been imposed on the body corporate collecting such information.

---

[14] In July 2017 it was reported that important personal information including social security numbers, birth dates, addresses, and in some cases drivers' license numbers, credit card numbers of around 147.9 million US citizens were breached due to the outdated technological safeguards used by the credit information company Equifax; See Equifax's Massive 2017 Data Breach Keeps Getting Worse, The Washington Post (1 March 2018) available at <https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect=on&utm_term=.03e306802d4e> (last accessed on 19 April 2018); In 2016 data from more the 412.2 million accounts on the Friend Finder's Network was breached by hackers due to weak data security protections, See Adult Friend Finder and Penthouse hacked in massive personal data breach, The Guardian (14 November 2016) available at <https://www.theguardian.com/technology/2016/nov/14/adult-friend-finder-and-penthouse-hacked-in-largest-personal-data-breach-on-record> (last accessed on 19 April 2018); In India, in early 2017 it was reported that personal information from McDonald's delivery app was leaked due to inadequate security features, See McDonald's India delivery app 'leaks users data', BBC News (20 March 2017) available at <http://www.bbc.com/news/technology-39265282> (last accessed on 19 April 2018).

[15] Rule 3, SPD Rules.

[16] Rule 4, SPD Rules.

[17] Rule 5(1), SPD Rules.

[18] Rule 5(2), SPD Rules.

[19] Rules 5(4) and (5), SPD Rules.

The SPD Rules require the prior consent of the provider of the information while disclosing sensitive personal data to a third party.[21] Transfer of sensitive personal data outside India is permitted on the condition that the same level of data protection is adhered to in the country, which is applicable to the body corporate under the SPD Rules.[22] The body corporate would further be deemed to have complied with reasonable security practices if it has complied with security standards and has comprehensive data security policies in place.[23]

While the SPD Rules were a novel attempt at data protection at the time they were introduced, the pace of development of the digital economy has made it inevitable that some shortcomings have become apparent over time. For instance, the definition of sensitive personal data is unduly narrow, leaving out several categories of personal data from its protective remit;[24] its obligations do not apply to the government and may, on a strict reading of Section 43A of the IT Act be overridden by contract. The IT Act and SPD Rules have also suffered from problems of implementation due to delays in appointments to the adjudicatory mechanisms created under the IT Act.[25] Some of these are not peculiarly Indian problems but endemic in several jurisdictions.

The deficiencies in regulation of data flows in India (and elsewhere in the world) is a consequence of a simplistic assumption that data flows are an unadulterated good. This is only partially accurate. It is clear that several data flows can cause considerable harm. But more significantly, the treatment of free data flows as an intrinsic good, as the recent exposé of data sharing practices by Facebook demonstrates, has placed the interests of the individual in whose name the information flows, as secondary to the interests of companies of various kinds which deal with the data. This gives a different complexion to the terminology in various jurisdictions designating the individual whose data is being collected as the ***"data subject"*** and the entity that collects the data as the ***"data controller"***. We begin by revisiting this terminology.

C. Data Principals and Data Fiduciaries

It is our view that any regime that is serious about safeguarding personal data of the individual must aspire to the common public good of both a free and fair digital economy.[26] Here, freedom refers to enhancing the autonomy of the individuals with regard to their personal data in deciding its processing which would lead to an ease of flow of personal data.

---

[20] Rule 5(7), SPD Rules.
[21] Rule 6, SPD Rules.
[22] Rule 7, SPD Rules.
[23] Rule 8, SPD Rules.
[24] Graham Greenleaf, India – Confusion Raj with Outsourcing in Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2017) at p. 415.
[25] Sreenidhi Srinivasan and Namrata Mukherjee, Building an effective data protection regime, Vidhi Centre for Legal Policy, New Delhi (2017) at pp. 18-19.
[26] Arghya Sengupta, Facebook's Brave New World, The Times of India (9 April 2018) available at: https://blogs.timesofindia.indiatimes.com/toi-edit-page/facebooks-brave-new-world-india-needs-strong-rules-to-ensure-internet-is-not-only-free-but-also-fair/ (last accessed on 17 May 2018).

Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated. In such a framework, the individual must be the ***"data principal"*** since she is the focal actor in the digital economy. The relationship between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust. Notwithstanding any contractual relationship, an individual expects that her personal data will be used fairly, in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship.[27] In the digital economy, depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals. This makes such entities ***"data fiduciaries"***.[28]

Pursuant to this, and as a general canon, data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy. It is our considered view that a regime based on the principles mentioned above and implemented through the relations described above will ensure individual autonomy and make available the benefits of data flows to the economy, as mandated by the TOR.

The twin objectives of protecting personal data while unlocking the data economy have often been seen as conflicting with each other.[29] Specifically, the TOR which mandates both these objectives, is said to have set up a false choice between societal interests and individual interests, a trade-off between economic growth and data protection.[30] It is argued that both are designed to achieve the constitutional objectives of individual autonomy, dignity and self-determination.

In our view, ensuring the protection of personal data and facilitating the growth of the digital economy are not in conflict and has rightly been pointed out, serve a common constitutional objective. However, each of them is motivated by distinct intermediate rationales — the former ensuring the protection of individual autonomy and consequent harm prevention and the latter seeking to create real choices for citizens. Both these intermediate objectives themselves are complementary — individual autonomy becomes truly meaningful when real choice (and not simply an illusory notion of it) can be exercised and likewise no real choice is possible if individuals remain vulnerable. The growth of the digital economy, which is

[27] Tamar Frankel, Fiduciary Law, 71(3) California Law Review (1983) at p. 795.
[28] This is taken from the view expressed by Jack M. Balkin, Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016) at p.1183.
[29] Elina Pyykko, Data Protection at the cost of economic growth?, European Credit Research Institute, ECRI Commentary No. 11 (November 2012) available at <https://www.ceps.eu/system/files/ECRI%20Commentary%20No%2011%20Data%20protection.pdf> (last accessed on 20 April 2018).
[30] See Submission by legal academics and advocates to the Justice Srikrishna Committee of Experts on Data Protection (31 January 2018) available at <http://privacyisaright.in/wp-content/uploads/2018/02/Detailed-Answers-to-the-Justice-Srikrishna-Committee-White-Paper-1.pdf> (last accessed on 20 April 2018).

proceeding apace worldwide, must be equitable, rights-reinforcing and empowering for the citizenry as a whole. In this, to see the individual as an atomised unit, standing apart from the collective, neither flows from our constitutional framework nor accurately grasps the true nature of rights litigation.

Rights (of which the right to privacy is an example) are not deontological categories that protect interests of atomised individuals;[31] on the contrary, they are tools that as Raz points out, are necessary for the realisation of certain common goods.[32] The importance of a right in this account is not because of the benefit that accrues to the rights holder but rather because that benefit is a public good that society as a whole enjoys. This is a critical distinction, and often missed in simplistic individual-centric accounts of rights.

This is an argument made most forcefully by Richard Pildes.[33] Pildes provides an example — in *Pico* v. *United States*,[34] the question before the US Supreme Court was whether a decision by a school to ban certain books from the library on account of them being "anti-American, anti-Christian, anti-Semitic and just plain filthy" violated the right to free speech of the students under the First Amendment. The decision to strike down the ban, Pildes believes, is justified not because the free speech right — in this case to receive information freely — is weightier than the state interest in promoting certain values in public education. Were this the case, it would be difficult to trammel the right to receive information freely at all. On the contrary, it was justified because the school could not remove books on the basis of hostility to the ideas that they contained — such reasons were illegitimate in this context where the common good is a public education system that differentiates politics from education. A decision on rights is thus a decision on the justifiability of state action in a given context that is necessary to serve the common good.

Thus the construction of a right itself is not because it translates into an individual good, be it autonomy, speech, etc. but because such good creates a collective culture where certain reasons for state action are unacceptable. In the context of personal data collection, use and sharing in the digital economy, it is our view that protecting the autonomy of an individual is critical not simply for her own sake but because such autonomy is constitutive of the common good of a free and fair digital economy. Such an economy envisages a polity where the individual is autonomously deciding what to do with her personal data, entities are responsibly sharing such data and everyone is using data, which has immense potential for empowerment, in a manner that promotes overall welfare.

---

[31] Ronald Dworkin, an influential legal philosopher, argues that rights of individuals against the state exist outside the framework of state sanctioned rights and act as trumps against the imposition of majoritarian decision-making. For details, see R. Dworkin, Taking Rights Seriously (Harvard University Press, 1978). The applicability of such a theoretical framework to actual constitutional practice is questionable. See Joseph Raz, Rights and Individual Well-Being, in Ethics in the Public Domain: Essays in the Morality of Law and Politics (Clarendon, 1995).

[32] Joseph Raz, Rights and Individual Well-Being, 5(2) Ratio Juris (1992) at p. 127.

[33] See R. Pildes, Why rights are not trumps: social meanings, expressive harms, and constitutionalism, 27(2) The Journal of Legal Studies (1998) at pp. 725-763.

[34] 69 U.S. 279 (1864).

Thus keeping citizens' personal data protected while unlocking the digital economy, as the TOR mandates, are both necessary. This will protect individual autonomy and privacy which can be achieved within the rubric of a free and fair digital economy. This is the normative framework that India, as a developing nation needs to assuredly chart its course in the increasingly digital 21st century.

D. Following Puttaswamy

This normative foundation of the proposed data protection framework is true to the ratio of the judgment of the Supreme Court of India in *Puttaswamy*.[35] The Supreme Court held that the right to privacy is a fundamental right flowing from the right to life and personal liberty as well as other fundamental rights securing individual liberty in the Constitution. In addition, individual dignity was also cited as a basis for the right. Privacy itself was held to have a negative aspect, (the right to be let alone), and a positive aspect, (the right to self-development.)[36] The sphere of privacy includes a right to protect one's identity. This right recognises the fact that that all information about a person is fundamentally her own, and she is free to communicate or retain it for herself.[37] This core of informational privacy, thus, is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves.

However, there may be other interests to consider, on which, the Court observed as follows:

> "*Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State.*"[38]

Thus, like other fundamental rights, privacy too can be restricted in well-defined circumstances. For such a restriction, three conditions need to be satisfied: first, there is a legitimate state interest in restricting the right; second, that the restriction is necessary and proportionate to achieve the interest; third that the restriction is by law.[39] As the excerpt from *Puttaswamy* above establishes, two points are critical — first, the primary value that any data protection framework serves must be that of privacy; second, such a framework must not overlook other values including collective values. In our view, the normative framework of a free and fair digital economy can provide a useful reference point for balancing these values in a particular case. To understand whether in a certain case, a right to privacy over that which is claimed exists, and would prevail over any legitimate interests of the state would depend on the interpretation by courts on how the needs of a free and fair digital economy

[35] 2017 (10) SCALE 1.
[36] See Bert-Jaap Koops et al., A Typology of Privacy, 38(2) University of Pennsylvania Journal of International Law (2017) at p. 566, as cited by Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 141.
[37] Her Majesty, The Queen v. Brandon Roy Dyment (1988) 2 SCR 417 as cited in *Puttaswamy* (2017) 10 SCALE 1.
[38] Per Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 179.
[39] Per Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1 at para 180.

can be best protected. It may happen by fully upholding the right, or alternatively finding the restriction justified, or a partial application of one or the other. The normative framework for this exercise is provided by the values of freedom and fairness. After all, freedom and fairness are the cornerstones of our constitutional framework, the *raison d'etre* of our struggle for independence.

E. Chapters in the Report

In order to ensure that a free and fair digital economy is a reality in India, there is certainly a need for a law that protects personal data. This report sets the framework for the contents of such a law and this could further be instrumental in shaping the discourse on data protection in the Global South.

Chapter 2 is a discussion of fundamental questions relating to scope and applicability of such a law. The question of scope of data protection laws in different jurisdictions is vexed — seamless transferability of data across national boundaries, has, for some, eroded the importance of the nation state.[40] While the factual premise of seamless transferability is largely correct, absent a global regulatory framework, national legislations supported by well-established conflicts of laws rules will govern issues relating to jurisdiction over personal data. In a legislation for India, questions of scope and applicability must be answered according to our policy objective of securing a free and fair digital economy. This objective will be severely compromised if data of Indians is processed, whether in India or elsewhere, without complying with our substantive obligations. Implicit in this is the ability of the state to hold parties accountable, irrespective of where data might have been transferred, and particularly to be able to enforce such obligations against errant parties. At the same time this objective cannot be enforced in derogation of established rules of international comity, respecting the sovereignty of other jurisdictions in enforcing its own rules.

Chapter 3 deals with the processing of personal data. Consistent with our view that the digital economy should be free and fair, the autonomy of the individual whose data is the lifeblood of this economy should be protected. Thus, a primary basis for processing of personal data must be individual consent. This recommendation is not oblivious to the failings of the consent framework. Consent is often uninformed, not meaningful and operates in an all-or-nothing fashion. This chapter provides an alternate framework of consent that treats the consent form, not as a means to an end, but rather as an end in itself. This imposes form and substance obligations on entities seeking consent as well as more effective mechanisms for individuals to track and withdraw consent.

Chapters 4 and 5 deal with obligations on data fiduciaries and rights of data principals. Anyone who uses personal data has an obligation to use it fairly and responsibly. This is the cardinal tenet of the proposed framework. We envisage the DPA and courts developing this principle on a case-by-case basis over time ensuring robust protection for individual data. At

[40] Jennifer Daskal, The Un-territoriality of Data, 125 Yale Law Journal (2015) at p. 326.

the same time, certain substantive obligations are critical if the objective of a free and fair digital economy is to be met. Specifically, these obligations ensure that the data principal is aware of the uses to which personal data is put and create bright line rules on when personal data can be collected and stored by data fiduciaries. This segues into Chapter 5 which deals with the rights of data principals. This is consistent with the principle that if the data principal is the entity who legitimises data flows, she must continue to exercise clearly delineated rights over such data. The scope of such rights, their limitations and their methods of enforcement are discussed in detail.

The flow of data across borders is essential for a free and fair digital economy. However, such flows cannot be unfettered, and certain obligations need to be imposed on data fiduciaries who wish to transfer personal data outside India. At the same time India's national interests may require local storage and processing of personal data. This has been dealt with in Chapter 6.

Chapter 7 discusses the impact of the proposed data protection framework on all allied laws which may either set a different standard for the protection of privacy or might otherwise authorise or mandate the processing of large amounts of personal data. Particularly, the impact on and necessary amendments to the IT Act, the Aadhaar Act and the RTI Act are discussed.

There are situations where rights and obligations of data principals and data fiduciaries may not apply in totality. This manifests in limited instances where consent may not be used for processing to serve a larger public interest such as 'national security', 'prevention and investigation of crime', 'allocation of resources for human development', 'protection of the revenue'. These have been recognised in *Puttaswamy* as legitimate interests of state. A discussion of such grounds where consent may not be relevant for processing is contained in Chapter 8. While some of the situations listed here only allow for processing without consent (non-consensual grounds), others are situations where substantive obligations of the law apply partially (exemptions). A critical element of this discussion relates to the safeguards governing such processing in order to prevent their wrongful use. Specific safeguards for both the grounds and the partial exemptions to the law are thus delineated together with the obligations that would continue to apply, notwithstanding such derogation from consent.

Critical to the efficacy of any legal framework is its enforcement machinery. This is especially significant in India's legal system, which has often been characterised as long on prescriptions and short on enforcement. This requires careful redressal. To achieve this, enforcement of this law must be conceived as having both an internal and an external element. External enforcement requires the establishment of an authority, sufficiently empowered and adequately staffed to administer data protection norms in India. However, we are cognizant of the limitations of a single authority to enforce a law of such significant magnitude, irrespective of whether it has nation-wide presence and resources. Consequently, any internal aspect of enforcement implies the need to formulate a clear legislative policy on *ex ante* organisational measures. Such policy and measures are to be enforced by codes of

practice to be developed in consultation with sectoral regulators, regulated entities and data principals, through an open and participatory process. Chapter 9 contains the details of the enforcement machinery under the proposed framework.

The report concludes with a summary of recommendations that we would urge the Government of India to adopt expeditiously in the form of a data protection law. A suggested draft of such a law has been provided along with this report.

F. Methodology

While framing the report, the Committee has conducted wide consultations. A White Paper was published by the Committee on 27 November 2017 for public comments. In addition, four public consultations were conducted by the Committee in New Delhi on 5 January 2018, Hyderabad on 12 January 2018, Bengaluru on 13 January 2018, and Mumbai on 23 January 2018. A number of views were expressed both in the written comments submitted to the Committee as well as oral representations at the public consultations. As will be evident from this report, such views, together with further research, have significantly informed our work, often departing from tentative viewpoints that may have been presented in the White Paper. This demonstrates the participatory and deliberative approach followed by the Committee in the task before it.

We are cognisant of the limitations of this report and lay no claims to exhaustiveness. The digital economy is a vast and dynamic space and we have consciously avoided wading into territories that do not strictly come within the framework of data protection issues set out in our TOR. Needless to say, such issues will have to be gone into at the appropriate time if our framework of a free and fair digital economy is to be truly upheld. Notably, these issues include those of intermediary liability, effective enforcement of cyber security and larger philosophical questions around the citizen-state relationship in the digital economy, all of which have been raised in public comments and committee meetings. Our deliberations have also raised questions related to non-personal data and emerging processing activities that hold considerable strategic or economic interest for the nation. Data processing is equally linked to the creation of useful knowledge, impinging values such as reliability, assurance and integrity. Many issues related to electronic communications infrastructure and services also arise in the larger context of the digital economy.[41] We leave such questions to the wisdom of a future committee in the hope that they will be duly considered.

G. Summary: A Fourth Way to Privacy, Autonomy and Empowerment

In our view, a combination of the elements outlined above would deliver a personal data protection law that protects individual privacy, ensures autonomy, allows data flows for a growing data ecosystem and creates a free and fair digital economy. In other words, it sets the

[41] See, for instance, UK Digital Economy Act 2017 (dealing with issues such as digital government, age verification and filters, universal service obligations related to internet speed, nuisance calls, copyright infringements and public service broadcasters).

foundations for a growing, digital India that is at home in the 21st century. This is distinct from the approaches in the US, EU and China and represents a fourth path. This path is not only relevant to India, but to all countries in the Global South which are looking to establish or alter their data protection laws in light of the rapid developments to the digital economy. After all, the proposition that the framework is based on is simple, commending itself to universal acceptability — a free and fair digital economy that empowers the citizen can only grow on the foundation of individual autonomy, working towards maximising the common good.

CHAPTER 2: JURISDICTION AND APPLICABILITY

Questions regarding scope and applicability are critical to any law, since they determine the extent of coverage of its rights and obligations. The issue of jurisdiction is the starting point since it answers two fundamental questions: first, whose interest the state seeks to uphold; second, why it is relevant for the state to uphold such interest. In the context of data protection, the borderless nature of the internet has challenged conventional views on jurisdiction and has often necessitated some form of extra-territorial application.

Every new law comes into force by intervening into existing practices, legal rules and conditions in a jurisdiction. For the effective implementation of the new rules, it is important to clarify the temporal applicability of the proposed framework as well as any provisions that allow for a smooth transition. As a result of these considerations, the chapter also deals with the issue of retrospective and transitional operation of any prospective data protection law.

A. White Paper and Public Comments

With respect to jurisdiction, the provisional view taken in the White Paper was to cover all instances of processing of personal data in the territory of India by entities having a presence in India.[42] With many companies not being based in India but carrying on business, or offering goods or services in India, it was also felt that the state had a legitimate interest in regulating such processing activities not entirely based in India or carried out by non-Indian entities that do not have a presence in India.[43] The Committee considered it worthwhile to extend the law to all entities processing the personal data of Indian citizens or residents; however it was felt that the law should not encroach upon the jurisdiction of other states which may have the effect of making the law a general law of the internet.[44]

A majority of the commenters were in favour of the law having some form of extra-territorial application. Covering foreign entities which deal with the data of Indian residents was stressed upon as necessary to ensure effective protection. However, the extent of such protection was varying with some suggesting expansive coverage, while others limited it to the formulation in the EU GDPR (i.e., entities offering goods and services in India). The commenters who argued against extra-territoriality did so largely on the basis of the impracticability of having to comply with competing obligations. As an alternative to extra-territorial application, a co-regulation model was suggested.[45]

---

[42] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

[43] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

[44] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 28.

[45] Comments in response to the White Paper submitted by Aditya Kutty of Uber India Systems Private Limited on 31 January 2018, available on file with the Committee.

On the further issue of the applicability of the law, transitional provisions were suggested in the White Paper to address the issue of retrospective application for ongoing processing.[46] Commenters largely agreed with this suggestion.

B. Analysis

I. Jurisdiction

(a) Conceptual Understanding of Jurisdiction

As is evident from the public responses, the scope of application of the proposed data protection law throws up several questions of principle and implementation. These questions are not unique to data protection — the nature of the internet as a seamless cross-jurisdictional network of accessible switches and pipes means that traditional concepts of territorial jurisdiction may require a rethink. This encompasses both substantive re-assessment of the meaning of territoriality, as well as a careful calibration of any extra-territorial application of a prospective law in concert with principles of international comity. In this process, the two principled objectives that must guide Indian thinking on the issue of application of the data protection law are as follows:

(i) Need to protect the personal data of persons present in India;[47]
(ii) Instituting a fair compliance mechanism for data fiduciaries who might operate in multiple jurisdictions; and
(iii) Establishing a domestic model that can be replicated by other jurisdictions such that each respects international comity.

Fortunately, this is not a greenfield subject. Legal scholars have, for a considerable period of time, debated the very same questions in the context of trying to understand the concept of jurisdiction. At its core, 'jurisdiction' is an exercise of power to define rights and obligations of parties.[48] Practically, the exercise of this power takes three forms — prescriptive, enforcement and adjudicatory.[49] Prescriptive jurisdiction refers to the power to make a law applicable to parties; enforcement jurisdiction is the supplementary power to enforce the law on the pain of penalty against parties; and adjudicatory jurisdiction is the power to judge the

[46] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 32.
[47] For example, in the EU data subjects who are "in the Union" are accorded protection, see Article 3(2) and Recital 23, EU GDPR.
[48] Arthur T. von Mehren and Donald T. Trautman, Jurisdiction to Adjudicate: A Suggested Analysis, 79(6) Harvard Law Review (1966) at p. 1126.
[49] See Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at pp. 765-773; See also Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000) at p. 139.

actions of parties, consequently determining rights and obligations.[50] At this stage, our interest is limited to the question of prescriptive jurisdiction alone, i.e., defining the legitimate scope of legislative power.

(b) Prescriptive Jurisdiction

Prescriptive jurisdiction has been understood in a seminal publication as capable of being exercised on five grounds:[51]

(i) Territoriality: Territorial jurisdiction is based on the occurrence of the cause of action within the borders of the state seeking to exercise jurisdiction over it. It is the fundamental public policy of each state to regulate actions in its territory based on the principle that any action that takes place in the territory, or any company that enjoys the benefits of the territory in carrying on business must be amenable to its legal framework.

(ii) Nationality: The nationality principle is based on the nationality of the alleged actor whose conduct has been called into question. The nationality principle is justified by the sovereign's interest in retaining control over the acts of its nationals wherever they may be.

(iii) Protective: The protective principle relies on the concept that a country should be able to protect its interests against acts abroad that have transnational effects. It requires jurisdiction to be vested to protect a security interest or the operation of the country's governmental functions, irrespective of where such interest lies.

(iv) Universality: The universality principle is based on the concept that all nations have an interest in combating certain trans-border crimes, such as piracy, slave trading, hijacking, etc.

(v) Passive Personality: The principle of passive personality permits a country to exercise jurisdiction over an act committed by an individual outside its territory because the victim is one of that country's nationals.

Related bases include objective territoriality and the effects doctrine,[52] wherein though acts might have been committed outside the territory of the state, they either have been completed in the state or have significant effects on the state thereby warranting the exercise of jurisdiction.[53]

---

[50] Arthur T. von Mehren and Donald T. Trautman, Jurisdiction to Adjudicate: A Suggested Analysis, 79(6) Harvard Law Review (1966) at p. 1125; A. Benjamin Spencer, Jurisdiction to Adjudicate: A Revised Analysis, 73 University of Chicago Law Review (2006) at p. 617; Adria Allen, Internet Jurisdiction Today, 22(1) Northwestern Journal of International Law & Business (2001) at p. 75.

[51] Jurisdiction with Respect to Crime, 29 American Journal of International Law (1935) at p. 519 (this was in the context of criminal law where several cross-jurisdictional questions were raised).

[52] Banyan Tree Holding v. Murali Krishna 2010(42)PTC 361.

[53] Christopher Kuner, Data Protection Law and International Jurisdiction on the Internet (Part 1), 18(2) International Journal of Law and Information Technology (2010) at p. 20.

(c) The Case for Data Non-Exceptionalism

It has been argued by several authors that data is un-territorial and thus traditional bases of jurisdiction described above are not easily applicable.[54] By virtue of being mobile, divisible, partitioned and location-independent, the nature of data challenges territoriality as the basis for exercise of jurisdiction.

This case for data exceptionalism has been questioned on various counts. First, any intangible asset such as intellectual property or debt has similar features to data in terms of being mobile (capable of being transferred or moved to offshore accounts) and divisible (in terms of being physically divided).[55] The law has established rules of jurisdiction for dealing with such assets. Second, data is not really as location-independent as it is posited to be. Even data on the cloud, actually physically resides on a server that is in the territory of a nation-state.[56] Once reduced to its physical form, exercise of jurisdiction appears to become a less complex exercise.

Third, much prior to the digital age, the possibility of transnational effects of domestic acts and *vice versa* were not unknown to the legal system. A decree against a defendant in one jurisdiction might lead to attachment of his properties in other jurisdictions if such property exists and none exists in the jurisdiction where the decree was passed. Similarly, regulations on trawlers by one country would affect the trawler no matter where it fishes. Neither of these actions prevents unilateral regulation by one state.[57] In the event that more than one state can exercise jurisdiction, a conflict-of-laws situation emerges, and courts will determine which country has the more 'substantial connection' to exercise jurisdiction. Similarly, for data which may not reside in one jurisdiction alone, an assessment of jurisdiction must be made in light of traditional principles that apply when an action has connections with multiple jurisdictions. It is not exceptional in terms of requiring a fundamental rethink of traditional legal formulations.

(d) Putative Bases for Jurisdiction

Jurisdiction over data, like other intangible assets is thus to be exercised to achieve the objectives listed above, using the twin parameters of state interest and fairness. India's interests mean that the following ought to be putative bases for exercising jurisdiction in a data protection law:

(i) All personal data of persons present in India that is processed must be protected. This can be ensured by exercising jurisdiction over personal data which is processed in India. If personal data is collected, disclosed, shared or

[54] Jennifer Daskal, The Un-territoriality of data, 125 Yale Law Journal (2015) at pp. 329-330.
[55] Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 735.
[56] Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 761.
[57] Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000) at p.136.

otherwise processed in India, the law will apply to the processing of such personal data irrespective of the following facts: where the fiduciary is incorporated; where the processing or any subsequent processing takes place. This is based on the principle of territoriality[58] and passive personality.

(ii) Personal data processed by Indian companies must be protected, irrespective of where it is actually processed. This is based on the principle of nationality as the company is located/incorporated within one's jurisdiction.

(iii) Personal data processed in India by foreign entities must be protected. Similar to the ground above, any processing in India is within the scope of Indian law on the basis of territoriality, irrespective of the nationality of the entity processing it.

While grounds (ii) and (iii) are straightforward, ground (i) is an exercise of long-arm jurisdiction.[59] This entails the state exercising extra-territorial jurisdiction on the ground that the actions elsewhere lead to significant effects in the state which require redressal. Such exercise, if resorted to by all states, might lead to a situation of considerable jurisdictional conflict. To prevent this, exercise of such jurisdiction must be carefully calibrated, keeping in mind the parameter of fairness. As a consequence, the following actions, despite being included on the basis of state interest, *ought to be excluded* from the application of the law:

a. **Irregular and ad hoc collection of data of persons present in India:** Despite attempts by some countries and private entities making the internet a walled garden for its citizens and consumers, the internet is free to access and use from any jurisdiction. This is central to our conception of a free digital economy. Thus, any website operating out of any foreign jurisdiction which is accessed by a person present in India may collect and process some personal data relating to such person. They should not be disincentivised from doing so.

   If such personal data is collected and further processed but is neither large-scale nor capable of causing significant harm in case of misuse, Indian law should not apply to this case. If this were to be done, every entity on the internet would have to comply with a plethora of laws on the basis of the off-chance that an individual from that country would access the service. To ensure the steady development of the internet as a freely accessible platform and treat data fiduciaries in other jurisdictions fairly, India should desist from making its law applicable to these instances. This would constitute an exception to putative bases (i), (ii) and (iii) discussed above. For example, a globally popular music streaming app is not available in India. However, some Indians may access it, either abroad or through usage of a virtual private

[58] Part of the cause of action in respect of transactions over the internet may occur in India even if there is no server in India involved. See World Wrestling Entertainment, v. M/S Reshma Collection & Ors 2014 SCC OnLine Del 2031

[59] Banyan Tree Holding v. A.S. Murali Krishna 2010(42)PTC 361; See Mark Gergen, Constitutional Limitations on State Long Arm Jurisdiction, 49(1) University of Chicago Law Review (1982).

network. This will not make the company subject to the Indian data protection law.

On the other hand, there may be cases of fiduciaries not physically present in the territory of India operating websites which must be regulated under Indian law. These include cases where such fiduciaries carry on business or systematically offer goods or service in India through the internet. This would go towards covering those entities that have a significant economic presence in India. Courts in India, while adapting conventional rules of jurisdiction to businesses carried on over the internet have distinguished between passive websites and others which target viewers in the forum state for commercial transactions resulting in harm in the forum state.[60] Recognising the nature of transactions over the internet, courts have interpreted the Trademarks Act and the Copyright Act to apply to persons not resident in India who nonetheless carry on business within the jurisdiction of the court.[61]

In addition to any link on the basis of systematic commercial activity, the law must also apply to activities such as profiling which pose considerable privacy harms which could be undertaken by fiduciaries that are not present within the territory of India. This would go towards covering those entities which have a significant digital presence for Indians though they may not have a significant economic presence. It is critical that such activities are regulated under Indian law.

An appropriate balance between these interests would be to restrict the application of the law in case of fiduciaries not present in India to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India.

b. **Processing of data that is not personal data of persons present in India by an entity in India:**

This is an exception to the principle of territoriality based on policy considerations of India having a large business process outsourcing industry handling large amounts of personal data of foreign nationals.[62] While the

[60] Banyan Tree Holding v. Murali Krishna 2010 (42) PTC 361 "This Court holds that jurisdiction of the forum court does not get attracted merely on the basis of interactivity of the website which is accessible in the forum state. The degree of the interactivity apart, the nature of the activity permissible and whether it results in a commercial transaction has to be examined". Further see Justice S. Muralidhar, Jurisdictional issues in Cyberspace, 6 The Indian Journal of Law and Technology (2010), **"**a lone trap transaction may not demonstrate the "purposeful" targeting by the defendant of the forum State or of "aiming" at particular customers therein. A more systematic behaviour over a series of transactions will have to be shown as having been entered into by the defendant."

[61] Icon Health and Fitnes, Inc. v. Sheriff Usman and Ors. 2017 SCC OnLine 10481 relying upon World Wrestling Entertainment v. M/S Reshma Collection & Ors 2014 SCC OnLine Del 2031.

[62] The IT-business process management sector revenues were estimated at around USD 130 billion in FY 2015-16 and USD 154 billion in FY 2016-17. The contribution of the IT sector to India's GDP stood at 7.7% in 2016. It is estimated that the sector will expand at a compound annual growth rate of 9.5% to USD 300 billion by

general principle of jurisdiction would require compliance with Indian law, to facilitate smooth continuance of business, an exemption may be provided to such industries on the condition that no personal data of Indians are collected or further processed there. This would constitute an exception to putative bases (ii) discussed above.

On this basis, the proposed law should apply to:

1. Processing of personal data collected, used, shared, disclosed or otherwise processed in India (Territoriality).
2. To ensure that the jurisdiction under clause (1) is not overbroad, personal data collected of persons present in India, directly by fiduciaries not present in India who are not carrying on business in India or offering goods and services in a targeted and systematic manner to persons in India, or processing personal data in connection with profiling of data principals in India, may be excluded;
3. Personal data collected, used, shared, disclosed or otherwise processed by Indian companies, irrespective of where it is actually processed. However, the data protection law may empower the Central Government to exempt such processors which only process the personal data of foreign nationals not present in India (Territoriality).

II. Retrospective and Transitional Application of the Data Protection Law

The time at which the data protection law comes into effect will have to take into account the twin interests of effective enforcement and fairness to data fiduciaries. It is thus commonsensical that the law will not have retrospective application, i.e. it will not apply to any processing activity that has been completed prior to this law coming into effect.

However, it is essential to keep in mind that if there is any ongoing processing activity at the time the law comes into effect, then the data fiduciary must ensure that it is in compliance with this law in relation to that activity. The subject matter of application of a data protection law is the processing of personal data and not personal data itself. This means that merely because some personal data has been collected prior to the commencement of the law, such personal data is not excluded from the application of the law. In this context, the term 'processing' is a broad term understood to include any kind of operation on personal data, ranging from complex analysis and indexing to mere storage. As long as such processing is ongoing after the law coming into force, it will be covered. On the other hand, if the processing is complete before the law comes into force, the law will not be applicable to such processing. For example, if a bank has retained the personal data of an account holder, the law will be applicable to such storage as soon as it comes into force. However, if the bank has deleted the personal data before the law comes into force so as to close the account, the law will not be applicable.

2020. See IT & ITeS Industry in India, Indian Brand Equity Foundation, available at <https://www.ibef.org/industry/information-technology-india.aspx> (last accessed on 23 April 2018).

At the same time, it must be noted that the data protection law is the first of its kind in India and involves the creation of an entirely new regulatory framework for the purpose of its enforcement. Thus, in imposing several obligations on data fiduciaries, it is important to provide enough time to facilitate the seamless application of the law. Further, several obligations created by the law require significant organisational changes in data fiduciaries. Therefore, the Committee is of the view that the law should come into force in a structured and phased manner. Provisions relating to the establishment of the DPA and its functions should come into force first, followed by most substantive obligations on data fiduciaries. Certain obligations however, such as requirements for storage and processing of personal data within the territory of India, may require longer time. Provision for such staggered enforcement will be made.

RECOMMENDATIONS

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. However, in respect of processing by fiduciaries that are not present in India, the law shall apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India. Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India. **[Sections 2 and 104 of the Bill]**

- The law will not have retrospective application and it will come into force in a structured and phased manner. Processing that is ongoing after the coming into force of the law would be covered. Timelines should be set out for notifications of different parts of the law to facilitate compliance. **[Section 97 of the Bill]**

CHAPTER 3: PROCESSING

Complementing the territorial application of the law is the question of its subject matter application. The chapter on territorial application is premised on the general principle that personal data of Indians is to be protected in a manner that prevents harm and promotes a free and fair digital economy. Harm, much like benefits, is a possible consequence of processing of data, understood in its broadest sense to mean its collection, storage, use, disclosure and sharing. The scope of the legal framework must thus cover all processing of personal data. Further, certain categories of personal data may be likely to cause greater harm, or harm of a graver nature. Such data, widely termed 'sensitive personal data' and needs to be delineated specifically.

To prevent harm from the processing of personal data, whether sensitive or otherwise, requires regulation of processing activities. In our framework, one central component of such regulation is the consent of the data principal. There are two principled advantages of consent — first, it respects user autonomy; second, it provides a clear basis for the entity to whom consent is given to disclaim liability regarding matters to which such consent pertains. However, consent on the internet today may not be entirely effective in allowing individuals to understand what they are consenting to. The dissonance between what consent is and what it ought to be in order to be normatively meaningful, is vast.

This report outlines a modified notice and choice framework that incentivises meaningful, informed consent being asked for and given. This includes related and critical issues of a child's consent and heightened safeguards for sensitive personal data processing. It is also imperative to recognise that the public good of the free and fair digital economy requires a consideration of collective benefits of data sharing, particularly in cases of legitimate state interest. Such consideration operates vis-à-vis both fiduciaries and principals.

In relation to data fiduciaries, there is an emerging need to recognise a new category of information as community data. This is information that is valuable owing to inputs from the community, which might require protection in addition to individuals' personal data. The outline for such protection concludes this chapter.

In relation to principals, data may be processed on certain grounds other than consent, where legitimate state interests exist. These might take the form of exemption to the rule of seeking consent alone or a wider exemption from substantive obligations in the law. Chapter 8 will outline these areas of non-consensual grounds of processing.

A. White Paper and Public Comments

With regard to issues of scope and applicability, the provisional view of the White Paper was that since the object of the law was to protect informational privacy rights, the law should

only apply to natural persons, and should cover both private and public sector.[63] Commenters were in favour of applying the law to only natural persons since juristic persons enjoyed other protections such as intellectual property rights, contractual rights, etc. While some commenters favoured treating the public and private sector at par, those who did not, argued on the basis of them performing different functions.

Personal data was defined by the White Paper as any data from which an individual is identified or identifiable or reasonably identifiable, with the identifiability capable of being both direct and indirect.[64] Thus any data relating to an individual, including opinions or assessments, irrespective of accuracy should be accorded protection.[65] With regard to processing of personal data, the White Paper argued for a broad definition that could incorporate new operations by way of interpretation.[66] It was however felt that the three main types of processing viz. collection, use and disclosure should be mentioned and the law should cover both manual and automated processing.[67] Further, it was felt that data controllers and processors should be separately defined and that imposition of obligations on data processors be weighed against compliance costs.[68]

Most commenters preferred the term 'personal data' with a broad definition to cover all types of data. One commenter pointed out that the law, like the law on intellectual property which was agnostic to quality, should be agnostic to accuracy and the law should specially cover opinions due to their ability to cause harm in the event of being inaccurate.[69] While commenters agreed that identification should be the standard for determining personal data, there was no consensus on what standard should be employed. Commenters preferred an inclusive definition of processing as opposed to an exclusive definition. There was also consensus on including both automated and manual modes of processing of personal data. With respect to defining entities such as 'data controllers' and 'data processors', there was significant divergence amongst commenters. Due to difficulties in defining such terms with

[63] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 32.
[64] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 39.
[65] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 39.
[66] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 46.
[67] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 46.
[68] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 51.
[69] Comments in response to the White Paper submitted by Sagnik Sarkar on 17 December 2017, available on file with the Committee.

precision, some commenters believed that all entities under the law should be carefully regulated.

Categories of data such as health information, genetic information, religious beliefs and affiliations, sexual orientation, racial and ethnic origin were considered as sensitive personal data by the White Paper.[70] The White Paper also recognised that processing of certain kinds of personal data due to the nature of the information had the likelihood of causing more harm to individuals and therefore required heightened levels of protection.[71] The commenters, for the same reasons, were in favour of including a category of 'sensitive personal data'. While there was no conclusive position with regard to what categories of personal data qualified as 'sensitive personal data', a significant number of commenters agreed with the suggestions in the White Paper. Some new categories were recommended including biometric data, passwords, trade union membership and Aadhaar number. Commenters suggested that there should be narrow grounds for processing of sensitive personal data. Additional safeguards for processing could take the form of technological and organisational safeguards.

The White Paper considered consent as a ground for the collection of personal data.[72] However, it was recognised that in practice, since consent could be used to disclaim liability, therefore the validity and meaningfulness of consent be carefully determined.[73] It was felt that consent should be freely given, informed and specific to the processing of personal data.[74] Notice was also viewed as an important requirement, since it operationalised consent.[75] Measures such as codes of practice, data protection impact assessments, data trust scores and consent dashboards were suggested as means to better employ notice requirements.[76] A large number of commenters opted for consent being the primary ground of processing, whereas an equal number argued that it be treated at par with other grounds. One commenter, however, argued that consent was not the only way to empower individuals due

[70] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 43.
[71] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 116.
[72] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.
[73] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.
[74] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 83.
[75] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 97.
[76] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed 20 April 2018) at pp. 97-98.

to the inapplicability of consent in some situations and presence of better alternatives.[77] In order to avoid consent fatigue, measures such as better notice design[78] and use of consent management architecture[79] were suggested.

The White Paper recognised children as a vulnerable group in need of a higher standard of protection.[80] Suggestions in this regard included parental authorisation for processing of personal data relating to children or only restricting such an authorisation for children of a very young age.[81] Alternately, the White Paper suggested that distinct provisions be carved out which prohibit the processing of children's data for harmful purposes.[82] A majority of commenters felt that the law should have special provisions to protect children's data, without being too paternalistic. Some did not comment on the issue, or were of the opinion that there was no need for special provisions since parental consent was sufficient to validate child's consent. Further, a majority of the commenters were unequivocal about there being no restrictions on prohibiting the processing of children's data or preventing them from accessing the internet due to free speech considerations.

B. Analysis

I. Building Blocks of the Law

(a) Personal Data

The breadth of protection that the law will offer depends on the definition of the term personal data. Since the 1980s, the standard for determining whether data is personal has been whether such data is related to an identified or identifiable individual.[83] Most jurisdictions studied by us employ some version of this formulation. The protection of any data that relates to an identifiable individual intuitively fits the objective of protecting an individual's identity.[84]

---

[77] Comments in response to the White Paper submitted by the Center for Information Policy Leadership on 31 January 2018, available on file with the Committee.
[78] Comments in response to the White Paper submitted by AZB & Partners on 31 January 2018, available on file with the Committee.
[79] Comments in response to the White Paper submitted by Joseph Hungin on 31 January 2018, available on file with the Committee.
[80] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.
[81] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.
[82] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 89.
[83] See 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 on 1 May 2018).
[84] *Puttaswamy*, (2017) 10 SCALE 1.

This standard of identifiability has served data protection very well over the years. However, developments in data science have considerably changed the understanding of identifiability.[85] Data no longer exists in binary states of identifiable or non-identifiable.[86] For instance, whether dynamic IP addresses constitute data about an identifiable individual depends on whether the person processing the data has additional data that enables the identification of the individual.[87] The degree of identifiability of an IP address may also be contextual in a different sense as several persons could be using the same machine. With advancements in technology, more and more identifiers of this nature are expected to emerge.[88]

A related challenge to identifiability arises from the failure of methods of de-identification.[89] Various studies have indicated in some circumstances that it may be possible to identify individuals from data sets which are seemingly anonymised.[90] Anonymisation refers to the process of removing identifiers from personal data in a manner ensuring that the risk of identification is negligible.[91] In some jurisdictions that were studied, such as the EU and South Africa, anonymised data falls outside the scope of data protection law.[92] Jurisdictions like the EU have also explicitly endorsed pseudonymisation,[93] a method by which personal identifiers are replaced with pseudonyms.[94] The manner in which the law should address these methods is also linked to the question of identifiability.

These concerns, however, do not necessarily lead to the conclusion that the standard of identifiability must be abandoned. In fact, despite the criticism, there is no alternative which provides a workable standard for demarcating data that must be protected under the law. In these circumstances, a definition of personal data centred on identifiability must be constructed with the full awareness that its scope will, in many cases, depend on the context

[85] Ira Rubenstien, Identifiability: Policy and Practical Solutions for Anonymisation and Pseudonymisation available at <https://fpf.org/wp-content/uploads/2016/11/Rubinstein_framing-paper.pdf> (last accessed on 11 May 2018); OECD, OECD Digital Economy Papers No. 229, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines available at < https://www.oecd-ilibrary.org/docserver/5k3xz5zmj2mx-en.pdf?expires=1526295425&id=id&accname=guest&checksum=27E40D67E438BF316639AB9B943AD5F0> (last accessed on 11 May 2018) at p. 10.

[86] OECD Digital Economy Papers No. 229, Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines available at <http://www.oecd-ilibrary.org/science-and-technology/privacyexpert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en> (last accessed on 11 May 2018) at p. 10.

[87] Patrick Breyer v. Bundesrepublik Deutschland, Court of Justice of the EU, Case C-582/14 (judgment dated 19 October 2016).

[88] Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at p. 1742.

[89] Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at p. 1742.

[90] Paul Ohm, Broken Promises of Privacy: Responding to the surprising failure of Anonymisation, 57 UCLA Law Review (2010) at pp. 1717 to 1722.

[91] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016).

[92] See Recital 26, EU GDPR; Section 6, POPI Act.

[93] Article 4 (5), Article 25 and Article 32, EU GDPR.

[94] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016).

in which the relevant data is being processed. Bearing this mind, we believe that a broad and flexible definition of personal data should be adopted.

Identifiability in circumstances where the individual is directly identifiable from the presence of direct identifiers such as names[95] is perhaps uncontroversial and will obviously be included within the scope of any definition of personal data. The definition should also, in addition, apply to contexts where an individual may be indirectly identifiable from data that contains indirect identifiers.[96] Whether indirect identification is possible is often a question of the means available to a data fiduciary and the nature of data available to the fiduciary to combine with the original data. The question of means could also be related to cost and prevalence of methods of analysis having regard to the state of technology. Thus, even where an individual is not directly identifiable, data about such an individual must be treated as personal if it is possible that he or she may be identified having regard to these factors.

Thus, the definition of personal data will necessarily have to be in the form of a standard capable of applying to various contexts in which the data of a person may be processed. However, expressing a definition in the form of a standard without clearly demarcating the kinds of data that are protected may not be sufficient. Flexibility in the definition should not be achieved at the cost of certainty. Here, the role of the DPA will be critical. From time to time, the DPA will have to offer guidance, explaining the standards in the definition as applied to different categories of data in various contexts, especially with regard to newer categories of data developed as a result of advances in technology.

A slightly different approach may be adopted with respect to de-identification, pseudonymisation and anonymisation. It must be acknowledged that there is no consensus on the meanings of these terms and commenters have noted that policy makers and on occasion, legislators have been imprecise in their use of these terms.[97] Polonetsky *et al* bring about a measure of clarity to these terms by analysing a spectrum of identifiability that has data that is obviously personal on one end and anonymised data on the other.[98] Pseudonymised data and de-identified data are inflection points on the spectrum nearer to anonymisation.

Anonymisation requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible.[99] In this aspect, anonymisation is distinct

[95] Polonetsky, Tene and Finch identify names, social security numbers and other basic contact information as direct identifiers in Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 605. See also definition of identifiable individual in Article 4 (1) of the EU GDPR for a list of identifiers.

[96] Date of Birth, Age gender, Zip Code etc. have been suggested to be indirect identifiers in Polonetsky, Tene and Finch Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 605.

[97] Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 596.

[98] Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 609.

[99] Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 618.

from de-identification which involves the masking or removal of identifiers from data sets to make identification more difficult.[100] Given the pace of technological advancement, it is desirable not to precisely define or prescribe standards which anonymisation must meet in the law. It is appropriate to leave it to the DPA to specify standards for anonymisation and data sets that meet these standards need not be governed by the law because they cease to be personal data.

A general standard in the definition of anonymisation regarding the possibility of identification, should be sufficient to guide the DPA in prescribing these standards. While the possibility of identification must be eliminated for a data set to be exempted from the rigours of the law, any absolute standard requiring the elimination of every risk including extremely remote risks of re-identification may be too high a barrier and may have the effect of minimal privacy gains at the cost of greater benefits from the use of such data sets.[101]

For other techniques of removing or masking identifiers from data including pseudonymisation, we adopt the term de-identification. The use of such techniques is encouraged and forms an important component of privacy by design. Despite the removal of identifiers from data, de-identified data carries with it a higher risk of re-identification.[102] Hence it is appropriate to continue to treat de-identified data as personal data. Here again, the precise standards that these processes must meet will be specified by the DPA from time to time. In addition to technical standards, this could also include specification of measures for safekeeping of the key or additional information that could lead to re-identification from pseudonymised data.

(b) Sensitive Personal Data

Most data protection legislations set out the rules or grounds in accordance with which personal data may be processed to prevent any harm to data principals. However, it has been observed that despite the existence of such rules or grounds, the processing of certain types of data (usually relating to an integral part of an individual's identity) [103] could result in greater harm to the individual. Consequently, processing of these types of data will require stricter rules or grounds in law to minimise such harm.

While there has been no clear-cut approach towards categorising sensitive personal data, some authors have suggested a contextual approach, i.e., where any personal data can become sensitive depending on the circumstances and the manner in which it is being processed.[104]

[100] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016) at p.16.
[101] Polonetsky, Tene and Finch, Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification, 56 Santa Clara Law Review (2016) at p. 619.
[102] Mark Elliot, Elaine Mackey, Kieron O'Hara and Caroline Tudor, The Anonymisation Decision-Making Framework (UKAN, 2016) at p.16.
[103] Edward J. Bloustein, Privacy as an Aspect of Human Dignity- An Answer to Dean Prosser (New York University, School of Law, 1964).
[104] Helen Nissenbaum, Privacy as Contextual Integrity, 79(11) Washington Law Review (2004).

However, this approach may place significant burden on data fiduciaries and regulatory resources as they would have to determine whether the personal data in question is sensitive or not, and whether it is capable of causing great harm to the individual, on a case by case basis. Therefore, by identifying certain types of data as sensitive in the law itself, and setting out specific obligations that must be met by the data fiduciary while processing such data, potentially significant harms may be pre-empted.

Data sensitivity, in one view, can depend on the legal and sociological context of a country.[105] However, certain categories of personal data are capable of giving rise to privacy harms regardless of context and an objective method of identifying such kinds of data becomes necessary. Hence, we have considered the following criteria to categorise what is 'sensitive':

(i) the likelihood that processing of a category of personal data would cause significant harm to the data principal;
(ii) any expectation of confidentiality that might be applicable to that category of personal data;
(iii) whether a significantly discernible class of data principals could suffer harm of a similar or relatable nature;[106]
(iv) the adequacy of general rules to personal data.

Based on the above criteria, the Committee has thought fit to categorise the following as sensitive personal data under a data protection law:

a. Passwords;
b. Financial data;
c. Health data;
d. Official identifiers which would include government issued identity cards;
e. Sex life and sexual orientation;
f. Biometric and genetic data;
g. Transgender status or intersex status;[107]
h. Caste or tribe; and
i. Religious or political beliefs or affiliations.

[105] See Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2(4) Journal of International Commercial Law and Technology (2007) at p. 191.
[106] Please note that these factors are adapted from those identified by Paul Ohm in Sensitive Information, 88 Southern California Law Review (2015) at p. 35.
[107] Personal data revealing the condition of a person as being transgender or intersex should be protected as sensitive personal data. The additional protection afforded by this categorisation is required due to the discrimination that they may be subjected to in society. Such persons are free to reveal their status voluntarily. We understand a transgender person to be one whose gender does not match the gender assigned to them at birth. On the other hand, an intersex person is one who is neither wholly female nor wholly male, or a combination of female or male, or neither female nor male (this may be due to physical, hormonal or genetic features).

However, a residuary power will be vested with the DPA to list out further categories of sensitive personal data on the basis of the above criteria. This power has been considered necessary due to the impracticability of laying down an exhaustive enumeration at the time of drafting. Harm can be caused by the processing of sensitive personal data *per se* or if it is aggregated for profiling. Consequently, the DPA will be granted a residuary power to list categories of sensitive personal data on the basis of both these sources of harm, as and when it considers necessary. Thus, for instance, geo-location data may be considered for listing as a category of sensitive personal data in the future since it may lead to harm upon aggregation.

II. Consent

The notice and choice framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded. It is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data.[108] Consent has been viewed as an expression of a person's autonomy or control, which has the consequence of allowing another person to legally disclaim liability for acts which have been consented to.[109] This is enabled through notice — an affirmative obligation placed upon data fiduciaries to communicate the terms of consent.[110] It should be understood that while notice as an obligation plays an important role alongside consent, it is also a crucial obligation even where processing takes place on the basis of grounds other than consent. Further nuances on the application of this obligation may be found in Chapter 4 and in Chapter 8 where the application to one of these grounds has been discussed.

A preponderance of evidence points to the fact that the operation of notice and consent on the internet today is broken.[111] Consent forms are complex and often boilerplate. Consequently, individuals do not read them; even if they attempt to, they might not understand them; even if they understand them, provisions to give meaningful consent in a granular fashion are absent.[112] Any enumeration of a consent framework must be based on this salient realisation: on the internet today, consent does not work.

---

[108] Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1049; Per Sanjay Kishan Kaul, J., in *Puttaswamy*, (2017) 10 SCALE 1 at p. 30 referring to the Second Circuit's decision in Haelan Laboratories v. Topps Chewing Gum. 202 F.2d 866 (2d Cir. 1953) penned by Judge Jerome Frank.

[109] Adam Moore, Toward Informational Privacy Rights, 44 San Diego Law Review (2007) at p. 812; Anita L. Allen, Why privacy isn't everything: Feminist reflections on personal accountability (Rowman & Littlefield, 2003) at pp. 115-16; John Kleinig, The Nature of Consent in The Ethics of Consent- Theory and Practice (Alan Wertheimer and Franklin Miller (eds.), Oxford University Press, 2009) at p. 4.

[110] Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p. 1031.

[111] Ryan M. Calo, Against Notice Skepticism in Privacy (and Elsewhere), 87(3) Notre Dame Law Review (2012) at p.1031; Reidenberg et al, Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11(2) Journal of Law and Policy for the Information Society (2015); Florian Schaub et al, A design space for effective Privacy Notices (Symposium on usable privacy and security, 2015) at p. 2; LF Cranor, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications and High Technology Law (2012) at p. 273.

[112] See B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

Despite these lacunae, individuals regularly consent to data collection and use practices as per the privacy policy or terms and conditions of the websites visited, applications downloaded, or programmes signed in to. So prevalent have such boilerplate contracts become in the online world, that courts too have often recognised their legal validity, irrespective of the unequal bargaining power of parties and doubts about how informed the giving of consent might have been.[113]

This has led to calls to do away with the individual's consent as a ground for processing completely[114] including in responses to the White Paper.[115] This conclusion is hasty. The problems with consent highlighted above relate to the efficacy of consent as a method of protecting personal data and consequently preventing individual harm. These are practical concerns rather than normative ones relating to the value of autonomy in a data protection framework. It would be inappropriate to dispense with the normative value of consent itself owing to the way in which it operates in practice currently. Rather, a modified framework for operationalising consent needs to be found.

(a) A revised operational framework for consent

If consent is still seen as a normatively significant expression of autonomy, the critical missing element in its operation is a revised operational framework for making such expression effective. The philosophical underpinnings of such a framework are provided by Arthur Leff in his seminal article 'Contract As Thing'.[116]

Leff contends that consumer contracts (of which online contracts are a manifestation) share no significant similarities with contracts *per se*- only one party sets the terms, with no opportunity for the other party to negotiate such terms; further, there is no 'bargain, agreement, dicker, process, mutability, becoming'[117] which are standard features of contracts. These 'contracts of adhesion' are not based on informed consent or mutual common understanding.[118]

He proposes instead to treat such contracts as 'things' *per se*, i.e., products. This would be in keeping with the limitations of contract law, which regulates the process of contracting,

[113] See for example, TradeComet.com LLC v. Google, Inc., 693 F. Supp. 2d 370, 377 (S.D.N.Y. 2010); Fteja v. Facebook, Inc., 841 F.Supp.2d 829 (S.D.N.Y. 2012).
[114] Daniel J Solove, Introduction: Privacy Self-Management and the consent dilemma, 126 Harvard Law Review (2013) at p. 1880; Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection- Discussion Document 2017-03, Takshashila Institution, (2017) available at <http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf > (last accessed on 23 March 2018).
[115] For instance, it was suggested that an accountability model should be adopted instead of consent being the primary ground of processing, see Comments in response to the White Paper submitted by the Takshashila Institution on 30 January 2018, available on file with the Committee.
[116] Arthur A. Leff, Contract As Thing, 19(2) American University Law Review (1970) at p. 131.
[117] Arthur A. Leff, Contract As Thing, 19(2) American University Law Review (1970) at p. 147.
[118] Andrew Robertson, The limits of voluntariness in contract, 29(1) Melbourne University Law Review (2005) at p. 179.

rather than the product at the end of it. Since a consumer contract is essentially a piece of paper over which there is no bargaining or agreement but merely evidence of the same, it is akin to a product which is exchanged at the end of the contracting process. Seeing an online contract in this manner allows us a wider operating arsenal to regulate notice and choice, i.e., the regime of product liability.[119]

(b) Consequences of such a Framework

The consequence of incorporating product liability into consent forms means that data fiduciaries will be liable, *as if* the consent form were a product.[120] This implies liability for any harm that is caused to a data principal pursuant to the latter providing consent, as a consequence of such processing.[121] Harms can ensue either from the data fiduciary not adhering to the terms of the notice or the notice itself being in a form which is not compliant with the data protection law.

The key illustrative harms that we have identified are:

(i) Such personal data is collected which are not those reasonably expected by the data principal;
(ii) Purposes for which personal data sought are not those reasonably expected by the data principal;
(iii) Disclosure and sharing of personal data is allowed with such persons and in such manner not reasonably expected by the data principal.

These would be analogous to traditional manufacturing defects in a product liability regime.[122] Further:

(i) Notice did not appear before application is installed;
(ii) Pre-checked boxes existed;
(iii) Appropriate standard of clarity of notice not met.

These would be analogous to traditional design defects in a product liability regime. Further:

---

[119] See David G. Owen, Products Liability Law (Thomson West, 2008); further, the Central Motor Vehicle Rules, 1989 that mandate compliance with minimum safety standards regarding automobile components are an illustration of the application of product liability in India. A key distinction however may relate to the possibility of withdrawal of consent in the case of data processing which may not be applicable in Leff's framework.

[120] The usefulness of the construct of "as if" as a technique of analysis by noted philosopher Kwame Anthony Appiah. See Kwame Anthony Appiah, As If: Idealisation and Ideals (Harvard University Press, 2017). For the benefits and pitfalls of such analysis, see Thomas Nagel, "As If", The New York Review of Books (2018) available at <http://www.nybooks.com/articles/2018/04/05/as-if-kwame-anthony-appiah/> (last accessed on 10 May 2018).

[121] Greenman v. Yuba Power Products, Inc (1963) 59 Cal.2d 57 [13 A.L.R.3d 1049]. The Supreme Court of California held that any entity involved in the chain of distribution for a defective product may be held liable for injuries caused by the defect.

[122] Wheels World v. Pradeep Kumar Khurana, I (2008) CPJ 324 NC; Tata Motors v. Rajesh Tyagi and HIM Motors Show Room, 2014(1) C.P.C.267.

(i) Potentially harmful/ burdensome/ onerous clauses of the contract were not pointed out specifically to the data principal.

This would be analogous to a marketing defect in a product liability regime.

Thus the substantive obligations on data fiduciaries in relation to the notice provided to data principals would *inter alia* be to:

1. Collect personal data necessary for providing service to the data principal to fulfil the purposes specified and disclose such data only to such persons as reasonably expected by the data principal.[123]
2. Communicate (1) above through a clear notice.
3. Ensure that contractual terms that are potentially onerous or harmful do not escape the attention of the data principal.[124]
4. Show notice before any such practices communicated in the notice take place.
5. Require affirmative consent from the data principal without any pre-checked boxes.
6. Provide requisite granularity thereby allowing data principals to access services without necessarily consenting to all or nothing.

(c) Enforcement of the Revised Framework

Enforcement tools relating to notice and consent will consist of the following:

(i) Model forms may be laid down by the DPA through codes of practice. Adhering to such pre-approved forms will demonstrate compliance with notice and consent related provisions in the law and no liability regarding these limited obligations will apply.[125] Needless to say, this will not affect substantive liability, if any, for other obligations under the law or contract. Some of the methods in which a notice can be improved have been illustrated in the guidance document for effective notice which is annexed as **Annexure B**.[126]

(ii) If a non-model form, not meeting the prescribed standards, is used then any liability for non-compliance with legal requirements shall be enforced on the pain of penalty.

[123] This is discussed in further detail in Chapter 4 of this report.

[124] Lord Denning's use of the red hand for potentially unreasonable clauses in a contract may be instructive here. A manicule may also be used. See J Spurling Ltd. v. Bradshaw, [1956] 1 WLR 461.

[125] This is similar to model Articles of Association in the Companies Act, 2013. Section 5 read with Schedule I, Table F of the Companies Act, 2013. Section 5(6): The articles of a company shall be in respective forms specified in Tables F, G, H, I and J in Schedule I as may be applicable to such company; Section 5(7), Companies Act, 2013 provides that a company may adopt all or any of the regulations contained in the model articles applicable to such company.

[126] The Committee would like to thank an independent graphic designer, Ananya Khaitan for designing this model notice.

(iii) Further, a data trust score (similar to a credit score) may be given to all significant data fiduciaries (a categorisation which has been outlined in Chapter 9), audited by data auditors and displayed prominently in the notice.

(iv) Dynamic consent renewal (opt-in, requiring fresh consent or opt-out requiring simple notification with option to opt-out) will be provided for, depending on the type of data in question. A consent dashboard may be created for this purpose.[127] The relevant provisions may be developed through delegated legislation by the DPA as and when it considers necessary.

(d) Standard of Consent

The revised notice and choice framework is a design modification which makes data fiduciaries communicate the terms of consent to data principals in a clear form with substantive obligations delineated. In our view, this is a significant step towards ensuring that consent is informed and meaningful.

A question however might arise regarding the standard of clarity that might be required in communicating consent. The EU GDPR mandates that the consent must be freely given, specific, informed and unambiguous for processing of personal data. Consent has to be expressed by a "statement or by clear affirmative action".[128] Certain jurisdictions are even more prescriptive, requiring particular font sizes, spacing, and more form-based conditions.[129]

While it is the Committee's view that the revised notice and choice framework as implemented through model forms prescribed by the DPA *per se* will provide sufficient clarity, the law will provide the conditions for validity of consent, requiring it to be 'free', 'informed', 'clear', 'specific' and 'capable of being withdrawn'. These conditions are discussed in greater detail below.

There are two standards of consent envisaged under the proposed data protection bill, regular or ordinary consent, and explicit consent.

The ordinary standard of consent as envisaged under the draft Bill needs to meet five conditions mentioned above. Firstly, it must be *free*. This is to be determined having regard to section 14 of the Indian Contract Act, 1872. Consent is said to be free when it is not caused by coercion, undue influence, fraud, misrepresentation or mistake, and meets any other conditions as per contract law jurisprudence.

Consent needs to be *informed*, having regard to whether it communicates relevant information in compliance with the draft Bill's provision on privacy notices.

---

[127] See Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016 for an instance of dashboard-based approach to consent in India.

[128] Article 4(11), EU GDPR.

[129] See Final Model Privacy Form under GLB Act (US) available at <https://www.ftc.gov/sites/default/files/documents/federal_register_notices/final-model-privacy-form-under-gramm-leach-bliley-act-16-cfr-part-313/091201gramm-leach.pdf> (last accessed on 26 April 2018).

Additionally, the consent needs be *specific*, having regard to whether the data principal can choose to not consent to certain purposes of processing of their personal data. If a particular type of personal data is not necessary for the performance of a contract, the enjoyment of a legal right, or the provision of a good or service, then such performance, enjoyment or provision cannot be made conditional to the giving of consent by the data principal. This makes the consent specific, in that it is unbundled from contracts and rights.

Consent also must be *clear*, having regard to whether it communicates agreement to the relevant processing through an affirmative action that is meaningful in a given context. Thus, silence and pre-ticked checkboxes would be unlawful modes of obtaining consent. However, that does not mean that in some instances that consent cannot be implied. For example, when an association's membership form requests for details such as name, address, telephone number, professional designation, and marital status, the affirmative action of entering such details can amount to a clear expression of consent. This would depend on the context in which the form has been collected, including whether the form explains the purposes of processing this data. Here, no explicit written expression of their agreement to such processing activity needs to be given separately.

Lastly, consent needs to be *capable of being withdrawn* as easily as it was given.

(e) Different Standards for Different Types of Personal Data Processing

The standard described immediately above must not be understood to be a one size fits all model for giving consent. While the ordinary standard must be applicable in the processing of personal data generally, there is a need to clarify where it may be permissible for consent to be implied. Large amounts of personal data may be collected and processed on a regular basis to maintain databases and for other instances of routine processing. In a limited set of such instances, implied consent may be sufficient while in others it may not be adequate. Where consent may be implied, it should nevertheless be free, informed, clear and specific having regard to the circumstances. Fixing these standards in the law does not rule out the use of implied consent in contexts where it is appropriate.

On the other hand, for processing of sensitive personal data, an even higher standard of consent than the ordinary one described above must apply. In some jurisdictions this has taken the form of requiring 'explicit consent' in the law.[130] This is a useful formulation.

Of the five conditions of valid ordinary consent described above, three are enhanced for the purpose of explicit consent. This makes the term a heightened form of ordinary consent, rather than merely the opposite of implied consent. The standard of explicit consent goes beyond the mode of communication of the agreement. This is described below.

[130] Examples of such jurisdictions include EU (Articles 9(1) and 9(2)(a)-(j), EU GDPR), Canada (Schedule 1, Section 4.3.4 and Section 4.3.6, Principle 3- Consent, PIPEDA), US FTC's Behavioural Advertising Principles in the United States, FTC Staff Report: Self-Regulatory Principles for Online Behavioural Advertising (2009) available at <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf> (last accessed on 27 April 2018).

Thus, to be *informed*, explicit consent should not just be in compliance with the provisions on notice under the draft Bill but must additionally draw the attention of the data principal to the purposes of, or operations in, processing activities that may result in significant consequences for her. While ordinary consent need only allow the data principal to choose between different purposes to be *specific*, explicit consent must additionally permit the choice between operations in, and different categories of, sensitive personal data relevant to processing. Finally, for explicit consent to be adequately *clear*, the expression of the consent should convey agreement to the processing objectively and without recourse to inference from conduct in a context. This would mean that if such an expression would not be meaningful in a different context, then it would not be adequate.

In the above example of an association's membership form, if the form also requires the collection of bank account details, then the mere act of entering data into the form cannot serve the purpose of expressing explicit consent. In order to meet the requisite standard of clarity, the data principal must not just enter the data, but must separately express that they consent to the relevant processing. A simple illustration of how this could be done is for her to write out her agreement to such processing. Other ways in which explicit consent can be expressed are by using a one time password (OTP). However, for this to be a sufficiently clear expression, the OTP provided to the data principal must be accompanied by a clear indication of what processing activity it would be authorising. Similarly, ticking a check-box which merely says 'I agree' would most likely not be considered explicit consent. However, it may be considered explicit if the check-box says 'I agree to the processing of the personal data entered above for the purpose of maintaining X Association's register of members, for communication of matters necessary for my membership in X Association and for transactions between the Association and myself.'

It is important to keep in mind that a large amount of personal data can be processed pursuant to the initial consent given by the data principal at the time of collection by the data fiduciary or any other party. Such consent will have to be as per the new framework and will be provided by the data principal for such processing as may be necessary to achieve the purposes for which consent is sought. The time for which such consent is valid is thus necessarily contingent on the purposes for which processing of personal data is sought. Where there are changes in such purposes or other relevant circumstances, the giving of such a sweeping consent would no more be adequate. In our view, the most efficacious mechanism for implementing ongoing consents is a consent dashboard.

(f) Consent Dashboard and Avoiding Consent Fatigue

A consent dashboard would enable data principals to keep track of consent for processing in real time and allow them to operationalise the right accorded to them under the data protection law. With the EU GDPR posing stringent requirements on data controllers to operationalise rights available to data subjects, various models for possible consent architectures that seek to enhance transparency have come up. For instance, Raschke *et al* envision two approaches. First, each fiduciary is required to operate its own dashboard; alternately, data principals have access to one dashboard operated by a third entity to manage

all fiduciaries they deal with.[131] A fiduciary-operated model is easier to enforce since the whole process of transfers can be logged and recorded internally. A single point dashboard while being more convenient from the perspective of data principals would require significant interoperability.[132]

A single point dashboard is akin to the one approved by the RBI in its Non-Banking Financial Company - Account Aggregator Directions.[133] The dashboard collects 'consent artefacts' of users, does not own any information but only provides information to the user in a consolidated manner. An aggregator that tracks consent, would thus only store the fact of the various consents given by the data principal to the different data fiduciaries and not ordinarily store any of the actual data.

We believe that comprehensive dashboards have significant potential in operationalising consent effectively. The opacity of consent and data sharing on the internet today is the foundation of several fears of data protection. Dashboards, if well implemented, can overcome this fear. However, if not carefully conceptualised and not made adequately simple, dashboards could become expensive white elephants.

Thus, for ease of enforcement, consent dashboards may be introduced in India in an incremental manner. The first approach where the fiduciary controls its own dashboard could be an initial step, while a central dashboard that coordinates with various fiduciaries can be introduced either sector-wise or universally over a period of time. This framework is recommendatory in nature and has been suggested to aid the resolution of the inherent problems of consent fatigue.

As a general comment, in much of the literature on notice and consent, critics of more robust protections use 'consent fatigue' almost like a slogan that brooks no disagreement. There is undoubtedly some truth in excessive consent requirements desensitising individuals towards consent. However this prospect only becomes real if it is envisaged that the principal will be continuously required to take affirmative action to demonstrate consent.[134] This is not an accurate factual premise in our framework. If data processing is in order to fulfil the purpose for which consent has been provided in accordance with law, one need not approach the individual for fresh consent. A notification may be sent to her via the dashboard of any processing necessary for fulfilment of such purpose. However, if personal data is used for other purposes, then fresh consent must be sought. If user fatigue ensues, then it is expected

[131] P. Raschke et al, Designing a GDPR-compliant and Usable Privacy Dashboard, Technical University Berlin, Germany (2017) available at <https://www.specialprivacy.eu/images/documents/IFIP-2017-Raschke.pdf> (last accessed on 26 April 2018).
[132] P. Raschke et al, Designing a GDPR-compliant and Usable Privacy Dashboard, Technical University Berlin, Germany (2017) available at <https://www.specialprivacy.eu/images/documents/IFIP-2017-Raschke.pdf> (last accessed on 26 April 2018).
[133] Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016.
[134] For instances of such criticisms, see B. W. Schermer et al, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, 16(2) Ethics and Information Technology (2014).

that data fiduciaries will, as responsible entities, not exacerbate such fatigue, and only use consent for purposes for which personal data is sought.[135]

This does not entirely obviate concerns of fatigue. While browsing websites, constant intimations for consent may affect user experience and desensitise individuals to privacy harms.[136] To be sure, processing of personal data may take place while browsing a website. In the offline world, this is akin to being under surveillance when walking into a shopping mall. For such regularly occurring situations, just as in the offline world, no explicit consent is usually taken, and the DPA may have to specify alternate standards of consent. At all points of time, such determination must be based on the *ex ante* assessment of potential of harm from such processing.

(g) Consent and Contractual Necessity

Data protection laws in some jurisdictions create a separate ground for processing personal data where it is necessary for the performance of a contract.[137] Recourse to such a ground would permit processing in relation to a contract entered into by the data principal, including contracts for the provision of goods and services. For instance, if an individual purchases a television set on an e-commerce website, the site would be justified in processing her personal data (name, address and credit card details) under contractual necessity to deliver the product. For the processing activity to be necessary for the performance of the contract there would have to be a direct nexus between the processing of the data and the execution of the contract.[138] In other words, the data fiduciary would have to justify that without processing of the personal data, the obligations under the contract cannot be performed.

As seen in such laws, the ground of contractual necessity is de-coupled or unbundled from consent in that a person cannot be later forced into consenting to processing of that personal data which is not needed by the other party in performing its obligations under a concluded contract.[139] If consent to processing is extracted by holding contractual rights hostage in this manner, such consent cannot be treated as free.[140]

---

[135] In user studies based on the existing legal framework in California, US, users showed little fatigue and preferred short, easy-to-understand, just-in-time notices, see A. McDonald & T. Lowenthal, Nano-Notice: Privacy Disclosure at a Mobile Scale, 3 Journal of Information Policy (2013).

[136] In an interesting study it was estimated that the national opportunity cost of reading privacy policies in the context of US was USD 781 billion, see A. McDonald and L. F. Cranor, The Cost of Reading Privacy Policies, 4(3) I/S: A Journal of Law and Policy for the Information Society (2008) at p. 544.

[137] See, for example, Article 6(1)(b), EU GDPR; Section 11(1)(b), POPI Act.

[138] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 (2018) at p. 8.

[139] The EU GDPR attempts to distinguish between consent and contract by ensuring that "the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract". Article 7(4), EU GDPR provides: "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." See also Recital 43, EU GDPR and Article 29 Working Party Opinion, Guidelines on Consent under Regulation 2016/679 (2018) at p. 8.

[140] Recital 43, EU GDPR.

Some laws, such as Canada's PIPEDA, do not set out such a ground.[141] This means that entities have to largely rely on consent for processing instead of any ground on contract. Since a person consents to a contract, it may appear intuitive that such consent is also the justification for the processing of personal data that is necessary for the performance of the contract.

On the other hand, it may be noted that once a contract has been entered into, a party may not prevent its execution without facing legal consequences. Once a data principal contracts to receive delivery of a good, it is implied that the other party would require personal data such as the delivery address so as to make the delivery. It may not appear meaningful to subsequently make the processing of such data contingent on the consent of the data principal. Enforceable contracts also allow parties to plan their own actions while relying on the certainty of each other's actions so as to secure the costs they incur. However, it is arguable that consent has to be capable of being withdrawn to be meaningful.[142] Such withdrawals, in the context of a contract, would prevent the other party from performing its obligations. Ordinarily, contracts do not permit unilateral withdrawals.

The Committee has noted these distinctions between consent and contract. However, there is considerable concern that a ground relying on contractual necessity could be easily misused. For one, a data fiduciary may insert clauses regarding various unrelated data processing activities within a contract and justify processing by claiming that it is necessary for the performance of those clauses. For another, it is unclear whether processing is subject to any meaningful check when the processing of personal data is the very subject matter of the contract or in digital contexts that have a pervasive connection with the personal data of a data principal. These contracts may be in a standard form, often entered into without any opportunity for negotiation.

Were a ground of contractual necessity to exist, there is a risk that data fiduciaries would be free to process any personal data if the processing is necessary to perform the obligations that the fiduciary may have inserted into the contract unilaterally. Where the essential objectives of a contract are not clearly defined, it may not be clear what personal data is and is not necessary for its performance. This could result in the treatment of such data as the "price" for a transaction. There continues to be some debate as to whether it is appropriate to permit the use of personal data as "counter-performance".[143]

---

[141] Clause 4.3, Schedule 1 and Sections 6.1 and 7 (1), (2), (3), (4) and (5), Part 1, Division 1, PIPEDA

[142] Recital 42, EU GDPR ("Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.")

[143] See, of instance, Article 3 of the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 2015/0287 (COD) available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015PC0634&from=EN> (last accessed 9 July 2018) (referring to "counter-performance other than money in the form of personal data or any other data.") Raising concerns regarding this formulation, the European Data Protection Supervisor has warned against "any new provision introducing the idea that people can pay with their data the same way as they do with money." See European Data Protection Supervisor, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (2017) available at

The Committee has attempted to mitigate these potential risks by opting to treat consent as the ground on which personal data is processed even where such data is necessary for the performance of a contract. However, where processing of personal data is necessary for a contract, the withdrawal of consent to such processing cannot be without consequences. If performance of the contract is sought to be refused, any legal consequences resulting from actions already taken by the other party in pursuance of the contract would have to be borne by the party preventing or refusing such performance.[144]

While we are aware that this does not entirely solve the problems outlined above, we consider this approach advantageous for two reasons. First, where a data principal consents to a contract that requires personal data processing, such consent would have to meet the heightened standard under data protection law instead of the lower standard of contract law. Second, even though contracts may not ordinarily envisage unilateral withdrawal, such withdrawals will be permitted in the context of personal data. The data principal will have the freedom to select which specific parts of their consent they would like to withdraw. As consent has to be "specific" to be valid, it would now also be possible to withdraw it specifically from a contract. Insofar as such a withdrawal would prevent the performance of a specific clause in a contract, the data principal would be able to choose to face the specific consequences that flow therefrom and choose what parts of the contract they would like the other party to continue performing. The data principal cannot be compelled through private law remedies to part with their personal data or go along with processing of personal data that has already been collected. This would be subject to the severability of such clauses from the rest of the contract and where this is not possible, the other party would be justified in seeking whatever damages may flow from the breach of the contract.

III. Protection of Children's Personal Data

It is widely accepted that processing of personal data of children ought to be subject to greater protection than regular processing of data.[145] The justification for such differential treatment arises from the recognition that children are unable to fully understand the consequences of their actions.[146] This is only exacerbated in the digital world where data collection and processing is largely opaque and mired in complex consent forms.

<https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf> (last accessed on 9 July 2018).

[144] See sections 39 (Effect of refusal of party to perform promise wholly) and 53 (Liability of party preventing event on which the contract is to take effect) of the Indian Contract Act, 1872.

[145] For instance, see COPPA, Article 8, EU GDPR., Sections 34 and 35 of the POPI Act.

[146] Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking?, 13(1) Professional School Counselling (2009); Michelle Sargent, Misplaced Misrepresentations: Why Misrepresentation-of-Age Statutes Must be Reinterpreted as They Apply to Children's Online Contracts, 112(2) Michigan Law Review (2013); Dale Kunkel, The Role of Research in the Regulation of U.S. Children's Television Advertising, 12(1) Science Communication (1990) at pp. 101-119.

Safeguarding the best interests of the child should be the guiding principle for statutory regulation on protecting data of children. This is enunciated in the CRC, to which India is a signatory.[147] The implementation of this principle in the data protection law should operate in two ways. First, it shall be a freestanding legal obligation on *all* data fiduciaries, i.e., principles will develop on how all data fiduciaries must process data relating to children in their best interests. Second, it should take the following specific form in relation to identified categories of data fiduciaries:

(a) Identification of guardian data fiduciaries

At present, the Committee understands that there are two categories of data fiduciaries who may be processing personal data of children: first, services offered primarily to children (e.g. YouTube Kids app, Hot Wheels, Walt Disney);[148] second, social media services (e.g. Facebook, Instagram).[149] The DPA shall have the power to notify data fiduciaries who operate commercial websites or online services directed at children, or who process large volumes of personal data of children as 'guardian data fiduciaries'.

(b) Who is a child?

In US, COPPA allows children 13 years of age and above to consent, whereas Article 8 of the EU GDPR mandates age 16 as the threshold, though allowing leeway for states to reduce the age of consent to 13. At the same time, the CRC defines a child as below 18 years of age under Article 1. This is also the age for anyone to validly enter into a contract in India as per Section 11, Contract Act.[150] The principled considerations for determining an age for consent are clear — protecting the child from harm while ensuring that she can autonomously participate in her own development.[151]

In order to determine the cut-off age, the choice should be governed by a balance of the following factors:

(i) Principled considerations;
(ii) The maximum age of 18 and the minimum age of 13 (considered as the relevant range in most literature and comparative jurisdictions);

[147] Article 3, CRC.
[148] Anthony Miyazaki et al, Self-Regulatory Safeguards and the Online Privacy of Preteen Children: Implications for the Advertising Industry, 38(4) Journal of Advertising (2009); Catherine Montgomery & Jeff Chester, Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework, 4 EDPL (2015).
[149] Sheri Bauman and Tanisha Tatum, Web Sites for Young Children: Gateway to Online Social Networking?, 13(1) Professional School Counselling (2009).
[150] Section 3, The Indian Majority Act, 1875 sets 18 as the age of majority. Under Section 11, Contract Act, persons who have attained the age of majority are competent to contract. In Mohori Bibee v. Dharmodas Ghose (1903) 30 Cal. 539 it was held that contracts entered into by minors are void ab initio. This position continues to remain valid today.
[151] Simone van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34(2) Wisconsin International law Journal (2016).

(iii) The need to prescribe a single threshold to ensure practical implementation.

At the moment, keeping in view the fact that the age for majority in the Contract Act is 18 and the provision of consent for data sharing is often intertwined with consent to contract, the age of 18 is recommended as the age below which a person is classified as a 'child' for the purpose of this law. We are aware that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high. However, consistency with the existing legal framework demands this formulation. Were the age of consent for contract to reduce, a similar amendment may be effected here too.

(c) Barred Practices

Certain types of data processing have been objectively found to be harmful for children. Harm, as used here, may be tangible (in terms of physical or reputational harm) or intangible (in terms of loss of autonomy). These include: behavioural monitoring, tracking, targeted advertising and any other type of processing which is not in the best interest of the child.[152] Guardian data fiduciaries must be barred from these practices insofar as it pertains to children.

To identify whether a service is being accessed by a child, the data fiduciary (including the guardian data fiduciary) shall adopt appropriate age verification mechanisms (mandatory login or date of birth input or other approved age verification mechanisms) and carry out processing on the basis of parental consent. An exception to any parental consent requirement would be a guardian data fiduciary that is exclusively engaged in the provision of counselling or child protection services to a child.

(d) Regulatory Approach

As is evident from the above scheme, the law will protect children's data in the following manner:

For guardian data fiduciaries, when providing services to children, certain types of processing that are harmful will be impermissible. Such data fiduciaries will have to incorporate appropriate age verification mechanisms and parental consent mechanisms.

For data fiduciaries, who are not guardian data fiduciaries, the special obligations (as specifically applicable to guardian data fiduciaries) will not be applicable. Such data fiduciaries will also be required to incorporate appropriate age verification mechanisms and parental consent mechanisms.

[152] Deborah Lupton and Ben Williamson, The datafied child: The dataveillance of children and implications for their rights, 19(5) New Media & Society (2017).

It is important to note that children constitute a large constituency of users of the internet (1/3rd of total internet users).[153] Since this is the case, a proportionate regulatory response would be to impose a general obligation to process personal data of a child in a manner that is in the best interests of the child. This principle can be developed further through codes of practice, standards and jurisprudence of courts of law.

We believe that the suggested approach is preferable to the current regulatory approach relating to children's data that is based *solely* on a system of parental consent. A dominant criticism against parental consent is that it is prone to circumvention, as it risks encouraging children to lie about their age, without necessarily achieving the intended purpose of protection.[154] Further, an overt reliance on parental consent may take away from the seriousness of the choice made by parents.[155]

Motivated by the need to protect children's personal data, we have imposed heightened obligations on guardian data fiduciaries who are barred from certain identified and harmful practices, along with processing permitted on the basis of parental consent. However, the proposed regulatory framework is not closed to incorporating improvements in the parental authorisation regime. These can become a part of the framework through codes of practice, as outlined above, providing greater flexibility in the development of the law to keep pace with technological advancement. The suggested framework sets up a regime that is in the best interests of the child.

IV. Community Data

Community data relates to a group dimension of privacy and is a suggested extension of our data protection framework. It is a body of data that has been sourced from multiple individuals, over which a juristic entity may exercise rights. Such data is akin to a common natural resource, where ownership is difficult to ascertain due to its diffused nature across several individual entities. It is relevant for understanding public behaviour, preferences and making decisions for the benefit of the community.

The difference between community data and other large-scale data collection lies in the degree of involvement of the larger community in building the body of data. It challenges the

[153] Dorde Krivokapic and Jelena Adamovic, Impact of General Data Protection Regulation on Children's Rights in Digital Environment, Year LXIV(3) Belgrade Law Review 3 (2016) referring to S. Livingstone et al., One in three: internet governance and children's rights, The Global Commission on Internet Governance, Paper Series No. 22 (2015); further, see The State of the World's Children 2017: Children in a Digital World, UNICEF (2017) available at <https://www.unicef.org/publications/index_101992.html> (last accessed on 11 May 2018).

[154] See Milda Macenaite and Eleni Kosta, Consent for processing children's personal data in the EU: Following in US Footsteps?, 26(2) Information & Communications Technology Law, at p.181. Parental consent, if implemented would also require the law to determine the age when parental consent expires and the individual's consent needs to be taken afresh. Why one particular age may be problematic has been pointed in the context of healthcare research where the child is progressively maturing, see M. J. Taylor et al, When can the child speak for herself? The limits of parental consent in data protection law for health research, Medical Law Review (2017).

[155] Catherine Montgomery & Jeff Chester, Data Protection for Youth in the Digital Age: Developing a Rights-based Global Framework, 4 European Data Protection Law Review (2015).

notion of individual control over her own personal data. Individuals may not be aware of what their data can disclose when aggregated with billions of other data points.[156] For example, Google Maps derives information about drivers' location, speed and itinerary through GPS enabled smartphones of numerous individuals.[157] This data is analysed by algorithms and produces reliable data on traffic flow across the world. Google Maps also collects information on places visited by individuals by asking them specific questions, which helps produce indicators like the availability of parking spots and washrooms, and popular hours at local stores.

Though these services are incredibly useful, two concerns arise. First, an individual's sharing of her personal data (such as current location) may lead to the sharing of similar personal data of her spouse, friends or family, without their consent.[158] Second, juristic entities make use of Big Data and can identify patterns of behaviour. This can have spill-over effects on the entire community as decisions may be taken on the basis of such patterns. Thus, community data may deserve protection.

A suitable law will facilitate collective protection of privacy by including a principled basis for according protection to an identifiable community that has contributed to community data.[159] This will take the form of class action remedies for certain kinds of data breaches involving community data with diffused social and systemic harm.[160] Tools like group communication and sanction may be envisaged. Such protection will take into account any intellectual property ownership of the juristic entity.

We strongly recommend that the Government of India considers such a law. It is our considered view, that not only individuals and communities, but in the near future corporate data too may require specific protection in the digital economy. Though the details of how such developments will take place, and indeed how community data will be protected will develop over time, acceptance of this principle may be seen as a peg on which such future developments may take place.

V. Entities to which the Law Applies

As is apparent from the scheme of this law, preventing privacy harms is essential for a free and fair digital economy. Such harm can ensue from processing by any entity, whether it be a government or a private entity. The ownership or structure of the entity is irrelevant for the purpose of this determination. On the contrary, the data that is processed, the reasons for such processing, and security standards maintained are the critical factors to determine the applicability of the law.

---

[156] Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 390.
[157] Patrick McDeed, The Big Data Driving Google Maps available at <http://ltd.edc.org/big-data-driving-google-maps> (last accessed on 22 April, 2018).
[158] See Neil M. Richards, The Dangers of Surveillance, 126 Harvard Law Review (2013) at p. 1939 as cited in Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 389.
[159] Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015) at p. 396.
[160] See Article 49, South Korean Personal Information Protection Act, 2011.

The question of whether the law will apply to the government or not is a red herring. It assumed relevance in light of the SPD Rules, which limited its applicability to body corporates. We do not see the reason for such a distinction to persist. Governments, as data fiduciaries, process large amounts of personal data, be it related to taxation, Aadhaar, social security schemes, driving permits, etc. Unlawful processing of such data can cause significant harm to individuals. All jurisdictions that we have considered in detail for our report have included the government; some like the US, have placed greater restrictions on it.

In our context, governments as data fiduciaries must be within the remit of the law. Ensuring that the state respects the right to privacy of the citizen should be a key aim of any data protection framework building on the fundamental right to privacy. In Chapter 1, we discussed the need to create a collective culture which values privacy. The state which collects and processes vast amounts of information of citizens must lead by example, as a data fiduciary, in creating such a culture.

At the same time, it must be recognised that several purposes for state processing of personal data may relate to the public interest. This may include processing for national security, investigating crime, protecting revenue etc.[161] Specific purpose-based exemptions for some of these categories must be created within the law. There may be other functions of the state where the relationship between the state and the citizen cannot be equated with that of a contractual relationship between private actors. These issues are dealt with in detail in Chapter 8 of the Report.

[161] These four were recognised by Chandrachud, J., in *Puttaswamy*, (2017) 10 SCALE 1.

RECOMMENDATIONS

- The definition of personal data will be based on identifiability. The DPA may issue guidance explaining the standards in the definition as applied to different categories of personal data in various contexts. **[Section 3(29) of the Bill]**

- The law will cover processing of personal data by both public and private entities. **[Sections 3(13) and 3(15) of the Bill]**

- Standards for anonymisation and de-identification (including pseudonymisation) may be laid down by the DPA. However, de-identified data will continue to be within the purview of this law. Anonymised data that meets the standards laid down by the DPA would be exempt from the law. **[Sections 3(3), 3(16) and 61(6)(m) of the Bill]**

- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law. **[Sections 3(35) and 22 of the Bill]**

- Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework which will apply a product liability regime to consent thereby making the data fiduciary liable for harms caused to the data principal. **[Section 12 of the Bill]**

- For consent to be valid it should be free, informed, specific, clear and capable of being withdrawn. For sensitive personal data, consent will have to be explicit. **[Sections 12 and 18 of the Bill]**

- A data principal below the age of eighteen years will be considered a child. Data fiduciaries have a general obligation to ensure that processing is undertaken keeping the best interests of the child in mind. Further, data fiduciaries capable of causing significant harm to children will be identified as guardian data fiduciaries. All data fiduciaries (including guardian data fiduciaries) shall adopt appropriate age verification mechanism and obtain parental consent. Furthermore, guardian data fiduciaries, specifically, shall be barred from certain practices. Guardian data fiduciaries exclusively offering counselling services or other similar services will not be required to take parental consent. **[Section 23 of the Bill]**

- The principle of granting protection to community data has been recognised by the Committee. This should be facilitated through a suitable law which is recommended to be enacted by the Government of India in the future.

CHAPTER 4: OBLIGATIONS OF DATA FIDUCIARIES

The obligations set out under a data protection law are critical to ensure the twin objectives of limiting processing to the fulfilment of purposes of data principals, while maximising gains from data processing for society at large. Failure to adhere to such obligations provides grounds to hold data fiduciaries accountable.

This chapter outlines the Committee's approach with regard to the various obligations that will be imposed on fiduciaries. Such obligations, many of which have been part of data protection principles since the FIPPs,[162] require careful adaptation with the emergence of new technologies of Big Data processing facilitated by AI and machine learning. While this report does not delve into the benefits and harms of such processing *per se*, it considers their relevance in devising a data protection framework that respects individual autonomy and upholds systemic fairness.

A. White Paper and Public Comments

The White Paper recognised purpose specification and use limitation as means to secure an individual's right to retain control over the manner in which her personal data is collected, used and disclosed.[163] It was felt that standards would have to be developed to guide data fiduciaries about the meaning of data minimisation in the context of collection and use.[164] While processing for incompatible purposes was considered to be impermissible, keeping in view the multi-functional nature of data, layered privacy notices, which provide further guidance on data use practice, were suggested instead of specifying use in a single privacy notice.[165] It was also recommended that use limitation may be modified on the basis of contextual understanding, therefore subsequent use may be permitted if it was in accordance with a reasonableness standard.[166]

A majority of commenters felt that the principles of purpose specification and use limitation were essential to avoid the misuse of personal data. However, opinions varied regarding the degree of alternate uses to be permitted, with some commenters opining that narrow definitions adversely impacted innovation, while others warned against vague and broad

[162] The FIPPs were first laid down in a report by the US Department of Health, Education and Welfare, See Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens Report (1973) available at <https://www.justice.gov/opcl/docs/rec-com-rights.pdf> (last accessed on 7 May 2018).

[163] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 109-110.

[164] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf?> (last accessed on 20 April 2018) at pp. 109-110.

[165] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp 109-110.

[166] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 109-110.

definitions as they failed to provide individuals with meaningful notice and consent. Most commenters believed that the processing of data should be allowed for compatible purposes and the use should be deemed compatible if it is reasonably connected to the overall activity of the data principal collecting such data. Commenters were in agreement with the White Paper's suggestion of a reasonableness standard i.e. processing can happen for purposes that a reasonably informed individual may expect.

The White Paper felt that the principle of storage limitation should find place in Indian law, however it was not feasible to specify precise time limits for storage of data. This would, instead, depend on the purpose for processing.[167] The White Paper also recommended use of terms such as 'reasonably necessary or necessary' to qualify the time period for storage and thereafter issuance of guidelines and court interpretation for clarity in implementation.[168]

A majority of commenters agreed with the White Paper's view on incorporating storage limitation. Most commenters believed that the law should contain a standard of reasonable necessity and time limits should be clarified through subsequent guidance. Commenters also suggested that with the advent of Big Data, new purposes may arise and therefore data could either be stored in anonymised form or renewal of consent could be obtained. Further, some commenters suggested that storage limitation not be imposed for meeting obligations of law and processing for historical, statistical and research purposes.

With regard to data quality, the White Paper took the view that it should be incorporated in Indian law. However, it was felt that the burdens imposed on the industry be balanced.[169] Use of terms such as 'reasonably necessary' was suggested to achieve the same.[170] All commenters agreed with the need to maintain data quality. However, most commenters were in favour of imposing the obligation of maintaining accuracy on data principals and felt that it would be an onerous task for the fiduciaries to ensure the same. The commenters also suggested that data principals have the right to correct inaccuracies in their data.

The White Paper was of the view that individuals be notified of data breaches where there was a likelihood of privacy harms being caused as a result of the breaches.[171] It was also suggested that the DPA be immediately notified on detection of breach. Further, too short a

[167] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.
[168] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.
[169] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.
[170] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 120.
[171] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

time for notifying the breach may be too onerous on small organisations and may prove to be counter-productive since there may be inadequate information about the breach and its likely consequences.[172] The format of the notification could be based on guidance issued by the DPA.[173] Some commenters were in favour of adopting the definition of personal data breach as provided in the EU GDPR, while others suggested the inclusion of confidentiality, integrity and availability breach in that definition. A large number of commenters were of the opinion that notification to the DPA in case of a breach should be mandatory. Comments with regard to the timeframe of notification varied from a reasonable timeframe to mandatory time spans. A few commenters also opined that notifying the DPA about every breach would overburden it, instead it should only be notified in case of major breaches.

B. Analysis

I. Fair and Reasonable Processing

In a fiduciary relationship, it is essential that the obligations of the fiduciary are clearly delineated. This is a corollary of the basic nature of such a relationship where the principal is dependent on the fiduciary for a particular service or achievement of an objective. The very existence of a fiduciary relationship is premised on the view that the relation between parties, and consequently the fulfilment of the objective by the fiduciary, may lead to an abuse of power.[174] While this may be true in any contract where contracting parties have unequal bargaining power, a fiduciary relationship is characterised by one party's dependence on another for performance of a service or achievement of an objective. Here, the law might deem it particularly necessary to intervene to prevent such abuse.[175] Thus the basic obligations to be followed by data fiduciaries in order to prevent abuse of power must be laid down in law.

All fiduciaries, irrespective of the exact nature of the contractual relation, must uphold trust and loyalty placed in them by the data principal.[176] This takes the form of a duty of care, i.e. to act in the best interest of the principal. Such a duty is mandated in order to ensure that no abuse of power ensues from the unequal nature of the fiduciary relationship.[177]

---

[172] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

[173] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 165.

[174] T. Frankel, Fiduciary Law, 71(3) California Law Review (1983) at pp. 809-810.

[175] Examples of fiduciary relationships could range from trustees, administrators and bailees in classical law to corporate directors and partners in the context of modern corporations and partnerships respectively. See T. Frankel, Fiduciary Law, 71(3) California Law Review (1983) at pp. 795-796. Further see, T. Frankel, Fiduciary Law (Oxford University Press, 2011).

[176] Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016).

[177] Jack M Balkin, Information Fiduciaries and the First Amendment, 49(4) UC Davis Law Review (2016) at pp. 1207-1208.

For a data fiduciary in the digital economy, abuse of power is understood as the data fiduciary processing personal data in a manner not authorised by the principal or law, for ends that may not be in the principal's best interest. The objective of preventing such abuse is best captured by an obligation to ensure fair and reasonable processing.

The obligation to process fairly implies that the data fiduciary must act in a manner that upholds the best interest of the privacy of the principal. Further, the obligation to process reasonably also implies that the processing must be of such a nature that it would not go beyond the reasonable expectations of the data principal. Ensuring fairness and reasonableness in processing are obligations that go beyond simply lawful processing on the basis of one of the grounds laid down in law. Placing such an obligation is recognition of the fact that given the unequal nature of the relationship and its inherent opacity, what is legal may not *ipso facto* be fair or reasonable.[178] Further it is testament to the fact that consent which may be valid for creating legal relationships may not be sufficient to fully disclaim liability.[179]

All personal data transfers in our framework must emanate from a legal ground (or a narrowly tailored exemption). For the obligation of fair and reasonable processing to be effective, it should be equally applicable to entities with whom the fiduciary might have shared data for fulfilment of the purpose, irrespective of whether such entity has a direct relationship with the individual or not. This can include data processors whose services may be necessary for carrying out the principal's purposes. Such data processors, who act on behalf of the data fiduciary, owe a similar duty of care to data principals in relation to processing as that owed by the said data fiduciary. This duty is owed regardless of the fact that the data processor does not control the objectives or ends of the processing and is only given a mandate by the data fiduciary.

Needless to say, the extent of the obligations of a data processor may differ, depending on the exact nature of processing in question and the requisite duty of care may be duly reflected in the contract between the data fiduciary and itself. This is precisely why laying down such a general principle of fair and reasonable processing will allow it to be developed by the DPA and courts of law, taking into account technological developments over time and differential obligations of different entities.

II. Purpose Limitation and Data Minimisation

[178] For instance, standard form contracts on the internet are an example, which while legal, may not always be fair due to the slim likelihood of the consumers reading and understanding the terms. See Robert A. Hillman, Consumer Internet Standard Form Contracts in India: A Proposal, 29(1) National Law School of India Review (2017).

[179] HLA Hart, The Ascription of Responsibility and Rights, 49 Proceedings of the Aristotelian Society (1949). See also Mindy-Chen Wishart, Undue Influence: Vindicating Relationships of Influence, 59(1) Current Legal Problems (2006).

Having established the general obligation on all fiduciaries, specific provisions to prevent abuse of power require detailing. To do this, the exact nature of legal relationships in the data economy need to be understood. The basic relationship is between two persons — the data principal and the data fiduciary. In this relationship, the data principal entrusts the fiduciary with personal data to achieve a particular purpose. This may involve, for instance, entrusting financial information to complete a transaction. The fiduciary undertakes to fulfil the purpose, whether itself or with the assistance of third parties. This relation, between 'principal and 'fiduciary' occurs at a mammoth scale in the data economy with over 16.1 zettabytes of data being generated in 2016.[180]

At its core, each relation between data principal and data fiduciary is undergirded by elements which characterise a classic fiduciary relationship: a data principal (data subject) entrusts personal data to a data fiduciary (data controller) for a particular purpose (financial transaction). If abuse of power is to be prevented, it is critical that the data fiduciary is obliged to use the personal data entrusted to it by the data principal only for the purpose for which the principal reasonably expects it to be used. This is the germ of the collection and purpose limitation principles. Both these principles seek to achieve the goal of data minimisation, as described in the White Paper.[181]

The purpose limitation principle has been the bedrock of data protection regimes for the last three decades.[182] It contains two sub-principles: first, that the purpose for which the personal data is processed must be clearly specified to the data principal (purpose specification); second, the processing must be limited to such purposes, or other compatible purposes (use limitation). Implicit in each of these sub-principles are two assumptions: first, that specification of purpose must meet a certain standard of specificity — simply specifying purposes in a vague manner will not be sufficient. Second, any unspecified use will be determined from the point of view of whether the processing is fair and reasonable in light of the purpose that was specified.

The first assumption is questionable. That purposes can be laid down with any degree of specificity is belied by existing practice in consent forms. By stating that the purposes for processing are 'improving consumer experience', 'for better services', etc. the principle is facially, though not substantively met. Yet, these may be valid, legitimate and lawful purposes. Further detailing of purposes in the interest of informing consent-giving, as is done

[180] It is estimated that by 2025 world's data will reach 163 zettabytes. It must be noted that not all data is personal data; see David Reinsel et al., Data Age 2025: The Evolution of Data to Life-Critical available at <https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> (last accessed on 7 May 2018).

[181] "The underlying logic of the use limitation and purpose specification principles is that of data minimisation, or the practice of limiting the collection of personal information to that which is necessary to accomplish a specified purpose". White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at pp. 105-106.

[182] For instance, see the EU GDPR, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), FIPPs (FTC, US).

by several data fiduciaries, might lead to long and unreadable consent forms, becoming counter-productive.[183] We are caught between the rock of vagueness and the hard place of incomprehensibility in trying to arrive at an appropriate standard of specificity.

Further, a limited set of future uses could be allowed to provide some degree of flexibility to the data fiduciary. This is based on the salient realisation that there may be other potentially beneficial uses of data which would not directly be at odds with the purpose specified to the data principal. Critically, such uses should be compatible, which has been understood to mean upholding the requirement of fairness.[184] The flexibility offered by this principle would permit use of the personal data for any other purpose by the data fiduciary which the data principal would reasonably expect having regard to the context and circumstances of processing of personal data. This is a commonsensical proposition, implemented by relating such uses back to the original purpose specified.

The purpose limitation principle is usefully seen in conjunction with another general principle, that of collection limitation. The principle of collection limitation mandates that only such data should be collected that is necessary for achieving the purposes specified for such processing. Thus, the minimum data necessary for achieving a purpose could be collected, and such data used only for the specified purpose and other compatible purposes and no other. Taken together, these are designed to lead to data minimisation that in turn, allows greater granular control for the data principal.

III. Big Data Challenges to Data Minimisation and Purpose Limitation

This belief of control through minimisation is a far cry from existing practice. Apart from the practices of vague purpose specification described above, the digital economy operates, not on the principle of data minimisation, but rather its antithesis, data maximisation.[185] This is particularly the case with the emergence of Big Data, processing vast amounts of data at scale to discern patterns of individual behaviour or market trends.[186] This is made possible by algorithms that enable machines to process at scale, learn from such processing, remember their learnings to gain intelligence and analyse such learnings constantly to generate useful results. These results are then used to more precisely target products, services, interventions to audiences now identified as receptive. Needless to say, such results are probabilistic,

[183] For instance, Gmail's privacy policy is a nine-page document that details the various purposes for which the data can be processed. See Google, Privacy Policy (2017) available at <https://static.googleusercontent.com/media/www.google.com/en//intl/en/policies/privacy/google_privacy_policy_en.pdf> (last accessed on 6 May 2018).

[184] UK Information Commissioner's Office, Big Data, artificial intelligence, machine learning and data protection available at <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> (last accessed on 6 May 2018) at p. 37.

[185] O. Tene and J. Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11(5) Northwestern Journal of Technology and Intellectual Property (2013) at p. 242.

[186] Big Data is characterised by three Vs, namely 'volume' which refers to massive databases, 'velocity' which refers to real time data and 'variety' which relates to different sources of data. See White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 8.

though their widespread use in the digital economy perhaps suggests that they are more often right than wrong.

Big Data processing is widely understood as comprising four stages: first, data collection from volunteered, observed, inferred or legally mandated data sets. This may or may not be limited to personal data sets; second, its storage and aggregation at scale; third, analysing such aggregated data through machine learning; fourth, its use for prediction or targeting.[187] Through these four stages, it is evident that data that is processed as well as the results from such data, may or may not relate to identified individuals. For example, Big Data analytics is widely used to predict weather patterns on the basis of large-scale processing of weather statistics as well as other relevant information.[188] At the same time, it is widely used in order to target products to particular individuals on the basis of their preferences derived from analysis of a large volume of diverse data sets.[189] Such targeting can be immensely useful - predictive text on searches brings down time spent on searches, responsive medical intervention ensures quicker emergency care[190] and tracking student performance and related data helps prevent dropouts.[191] Equally, Big Data analytics may also lead to tangible harms to individuals when targeting goes awry. Since the nature of Big Data analytics is probabilistic, incorrect targeting may lead to inaccuracy of personal data, ensuing denial of service and discrimination. Examples of such harms abound.[192]

An assessment of the relative benefits and harms of Big Data processing is orthogonal to our report. The benefits of such processing must outweigh its harms for such processing to become widely accepted and used by fiduciaries. That appears to be the case. Tim Wu writes about how the business model of the entire digital economy appears to be founded on free services and the use of personal data for targeted advertising.[193] It need not have turned out

[187] International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics (2014) available at <https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2014/06052014_en.pdf> (last accessed on 6 May 2018) at pp. 4-5.

[188] UK Information Commissioner's Office, Big Data, artificial intelligence, machine learning and data protection available at <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> (last accessed on 6 May 2018) at p. 10.

[189] Orcan Intelligence, Big data analytics is used by companies such as Netflix to adjust content and personalize the user-experience, see How Netflix uses Big Data (2018) available at <https://medium.com/swlh/how-netflix-uses-big-data-20b5419c1edf> (last accessed on 6 May 2018).

[190] According to recent research, data from fitness trackers could help predict the risk of a heart-attack, see S. Davila et al, Beyond Fitness Tracking: The use of consumer-grade wearable data from normal volunteers in cardiovascular and lipidomics research, PLoS Biol 16(2): e2004285.

[191] See D. West, Big Data for Education: Data Mining, Data Analytics, and Web Dashboards, Brookings (2012) available at <https://www.brookings.edu/wp-content/uploads/2016/06/04-education-technology-west.pdf> (last accessed on 06 May 2018).

[192] For instance, the insurance company Progressive required customers to install a monitoring device in their cars through which customers who drove infrequently and avoided driving during the night were given better rates on the basis of the assumption that such driving practices reduced the risk of accident. However, this ended up discriminating against late-night shift workers who were largely from minority communities. For further reading see The Center of Internet and Society, Benefits and Harms of "Big Data" (2015) available at <https://cis-india.org/internet-governance/blog/benefits-and-harms-of-big-data> (last accessed on 6 May 2018).

[193] This is described as nano-targeting. Tim Wu, The Attention Merchants: The Epic Scramble to get Inside Our Heads (Vintage Books, 2016) at p. 296-302.

this way and need not continue this way if significant harms ensue as a result of erroneous targeting. It is a choice that businesses have made, and individuals have consented to, if not positively supported. This is neither the time nor place to question this development, except to retain a healthy scepticism of whether a "free internet" is, or will remain, welfare-maximising for individuals.

For the purposes of a data protection framework, Big Data processing presents a frontal challenge to the well-established principles of collection limitation and purpose limitation. The basis for processing at scale is the collection of large amounts of personal data and its subsequent use for a variety of purposes. Particularly, the challenges are twofold: first, the uses to which personal data are put often only become apparent over time. This is because several uses are derived only after an assessment of the personal data from a collection of data sets from different sources, which may not have been intended to combined.[194] As a White House Report on Big Data and Privacy[195] notes even the algorithm that is used to process such data resulting in potential future uses may not be in existence at the time of initial collection. Second, these uses may be a result of re-identification of individuals from anonymous data sets. The increasing ease of re-identification means that at the time personal data was collected and notice was provided on uses, such future uses based on re-identification could not have been envisaged.[196] Thus limiting collection is antithetical to large-scale processing; equally, meaningful purpose specification is impossible with the purposes themselves constantly evolving.

In order to ensure that any such use of big data analytics is narrowly tailored and geared towards maximising individual benefits and minimising harm in the digital economy, it is necessary to constrain its uses in ways that optimally respect individual autonomy in a free and fair digital economy. This is possible in the following three ways:

First, to the extent possible, anonymised data can be used which cannot later re-identify an individual. This ensures that the benefits of Big Data processing can continue together with the protection of individual autonomy.

Second, Big Data processing that is used to improve the provision of the service or purposes reasonably expected by the principal, should be permitted to continue. There is no adverse effect on autonomy by the use of a technique (large scale data processing), on the contrary, such use may well be within the reasonable expectation of the principal and presumably for her benefit.

Third, when Big Data processing is used for repurposing, with unknown future purposes which could not have been reasonably communicated to the data principal at the time of

[194] Nancy King and Jay Forder, Data analytics and consumer profiling Finding appropriate privacy principles for discovered data, 32(5) Computer Law and Security Review (2016) at pp. 699-700.
[195] Executive Office of the President, President's Council of Advisors on Science and Technology, US, Big Data and Privacy: A Technological Perspective (May 2014) at p. ix.
[196] Nancy King and Jay Forder, Data analytics and consumer profiling Finding appropriate privacy principles for discovered data, 32(5) Computer Law and Security Review (2016) at p. 704.

collection, then collection limitation and purpose specification might not be possible in the form in which it is set out in the law. Narrow tailoring of the use of personal data requires the following substantive conditions to be met:

(i) Personal data should not be processed in a manner that gives rise to a risk of significant harm to any data principal. This ought to function as a general obligation on any fiduciary that engages in any repurposing according to subsequent purposes that could not be reasonably communicated at the time of collection.

(ii) Personal data may be processed in a manner that does not take any decision specific to, or action directed specifically at, any individual. This can take the form of analysis of general trends or patterns. Since there is no possibility of individual harm which flows from such usage, it should be permitted to continue. Processing subject to this condition has been discussed further in Chapter 8 under 'Research Activities'.

(iii) If, however, personal data is used to take any decision specific to, or action directed specifically at any individual, then explicit consent of the individual in accordance with the law is to be taken. This is necessary to uphold individual autonomy such that any use of personal data to take any action that impacts a data principal must be processed on the basis of her consent. Further, for any data fiduciary who wishes to engage in such processing, certain organisational obligations must be adopted. These include, but are not limited to, a data trust score, regular data audits, a DPO and a transparent mechanism for data processing which allows the individual access at any time to the personal data held by a fiduciary with an option to correct such personal date for inaccuracies.

It may be argued that seeking such consent may be un-implementable. We do not see why this must be the case — if an individual can be targeted precisely for the purpose of showing her an advertisement or a particular communication, surely, she can be targeted for seeking consent before such action. The final call on how the consent should be obtained should be left to the determination of the DPA.

Such repurposing should only be permitted if such later purposes could not have been known at the time of collection and could not reasonably be communicated to the individual. If such knowledge of purpose is objectively possible and necessary communication of the same to the individual has not been done, such initial processing should be made unlawful and appropriate enforcement action may be taken by the DPA.

It is our view that in this manner, the interests of individual autonomy can be optimally protected in creating a free and fair digital economy. The above discussion is in the nature of recommendations to the Central Government which may be taken up at an appropriate time.

IV. Transparency

In securing their rights under data protection law, a prime barrier faced by data principals is the lack of information on how their personal data comes to be processed. Especially in the digital context, it becomes difficult for a data principal to know and understand whether, by whom and for what purpose personal data about her is being collected and processed.[197] In this regard, it is essential that processing be carried out transparently. This not only bolsters the fairness of the processing activities, ensuring that data principals can trust them, but also makes sure that data fiduciaries are accountable by creating some scope for principals to challenge them.[198]

As a result of this, a principle of transparency is incumbent throughout the life cycle of a data processing activity from the time the data is collected to various points in the interim. It has thus been integrated into our proposed framework at various points. Most prominently, a data fiduciary is obliged to provide *notice* to the data principal no later than at the time of the collection of her personal data. If the data is not being collected from the principal directly, this obligation is still applicable, and the fiduciary must provide the notice as soon as is reasonably practicable. The information that a fiduciary is required to disclose to the data principal has been specified to ensure that it alleviates, as best as is possible, the problems of opacity, uncertainty, lack of clarity, and lack of accountability because of which privacy harms are caused. Not only must the data principal be informed as to who is processing what personal data of theirs for what purposes, they must also be told various points of relevant information including the basis of processing, their ability to withdraw consent (if processing is based on consent), any legal obligations on the basis of which the processing is taking place, persons with whom the data may be shared, the period of retention of data, as well as the procedure for the exercise of data principal rights, the procedure for grievance redressal and the right to file complaints with the DPA.

These points of information must be conveyed to the principal in all circumstances except where processing is taking place for emergency situations requiring prompt action. It must also be ensured that the form of the communication is clear and concise so that it is easily comprehensible. There may also be various situations where it is necessary for the information to be communicated in multiple languages.

[197] Recital 58, EU GDPR (identifying the "proliferation of actors and the technological complexity of practice" as being especially problematic reasons for such difficulty).
[198] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (2018) at p.5.

Transparency requirements may also be seen in various obligations regarding the manner in which the data fiduciary is to communicate with the data principal in relation with the exercise of any of the data principal's rights (described in Chapter 5). Thus, for instance, the fiduciary is required to acknowledge receipt of requests for the exercise of such rights and clearly communicate adequate reasons for the refusal of any right. Apart from this, the data fiduciary is also required to maintain transparency regarding its general processing activities and practices, making available such information for any data principals seeking clarity on the same at any point of time. This obligation to publicise general practices regarding data processing may be seen as a practice that some entities already follow in the form of organizational privacy policies that may be available on their websites or otherwise placed in prominent locations.

V. Organisational Obligations on Data Fiduciaries

This report has thus far been based on the premise that a free and fair digital economy is possible when the individual, whose personal data is at the core, is the key lever for all data transfers. We are cognisant that such vision is remote from the functioning of the digital economy today where the individual is only notionally in control of her own personal data. Thus, trust in data fiduciaries, particularly today, requires such fiduciaries to take certain organisational measures to ensure that personal data is processed lawfully, fairly and reasonably and not wait for individuals to *ex post* identify non-compliance.

In academic literature, such organisational measures have been described as involving the setting up of an accountability framework for data fiduciaries.[199] In our view, organisational measures are critical components to ensure that data fiduciaries fulfil their obligation of fair and reasonable processing and are in a position to demonstrate such fulfilment when called upon to do so. The enforcement of such obligation may either take place by an assertion of individual right, or, through appropriate audit mechanisms and regulatory action.

This framework has been implemented within a rights-based approach in the EU GDPR. The EU GDPR imposes an accountability obligation that requires data controllers to comply with all obligations under EU GDPR and be able to demonstrate this compliance.[200] This requires the implementation of concrete organisational measures to operationalise data protection principles. It is our view that a general obligation to undertake organisational measures to ensure fair and reasonable processing needs to be placed on all data fiduciaries.

[199] In a consent-based framework the data principal is responsible for being aware of the terms of the data access to which she has consented to as opposed to an accountability model where the burden of compliance with obligations is imposed on the fiduciary by the regulator. See Rahul Matthan, Beyond Consent: A New Paradigm for Data Protection, The Takshashila Institution (2017) available at <http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf> (last accessed on 6 May 2018); Further see Comments submitted in response to the White Paper by The Takshashila Institution on 30 January 2018 available on file with the Committee.

[200] The Article 29 Data Protection Working Party recommended the inclusion of the principle of accountability in the European Union's data protection regime, see Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (2010). Further, see Article 5(2), EU GDPR.

Regarding the content of such organisational measures, it is our view that they should be carefully calibrated to the nature of the processing which takes place. Thus, for all data fiduciaries, baseline minimum obligations need to be imposed. These include implementation of appropriate security measures and mechanisms for individuals to access their personal data. For significant data fiduciaries, heightened organisational measures need to be taken. These organisational measures have broadly been described as 'privacy by design' that establishes data handling practices in the organisation in a manner ensuring compliance with the law by minimising or eliminating adverse impacts on privacy.[201] This may also ensure cost effective compliance with the obligations under the law. For instance, the EU GDPR refers to the adoption of technical and organisational measures that take into account the rights of individuals while designing policies to ensure that they can effectively meet their obligations under the data protection law.[202] A list of such practices, which we hope will develop further through codes of practice, has been devised and submitted to us.[203] We urge the DPA to consider these and other best practices to lay down precise obligations for data fiduciaries so as to ensure strict compliance with the law. In this exercise, it is recommended that the DPA conduct capacity building exercises to create skilled professionals in order to implement a 'design-thinking' approach. Industry bodies can also play a pivotal role by assisting the DPA in this process.

A critical obligation which requires specific highlighting here is access control obligation. Access control obligations are designed to ensure that all data accesses are legitimate and that they do not violate consent, purpose limitation or any other substantive provision. This will require all data processing and access requirements to be scrutinised *apriori* and *ex post* through audits. The data fiduciary and any associated processors should maintain non-repudiable logs (perhaps in a blockchain) of all requests and approvals. It must be ensured that data access is according to the authorisations granted. *Ex post* audits are, in any event, possible.

VI. Storage Limitation

The principle of storage limitation, which is closely connected to the principle of purpose limitation, envisages that data should be stored by the fiduciary only for a time period that is

[201] The principles of 'privacy by design' were developed by the Privacy Commissioner of Ontario, Canada and focus on making privacy assurance an organization's default mode of operation, see Privacy Commissioner of Ontario, Canada, Privacy by Design (2009) available at <https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf> (last accessed on 7 May 2018).

[202] Recital 78, EU GDPR.

[203] Email Response submitted in response to the White Paper by the Centre for Information of Policy Leadership on 30 January 2018, available on file with the Committee. There are also numerous examples of sector-specific codes of practice, for instance See UK Information Commissioner's Office, The Employment Practice Code available at <http://www.pdpjournals.com/docs/99007.pdf> (last accessed on 12 May 2018); German Data Protection Principles for Connected Vehicles (Vehicles connected to the internet) (2014) available at <http://www.pdpjournals.com/docs/99009.pdf > (last accessed on 7 May 2018) etc.

necessary to fulfil the purpose for which it was collected.[204] Once the purpose has been achieved, the data should be deleted or anonymised. The rationale behind this is that once processing is over, control over the data may be lost, since it is no longer of any interest to the data fiduciary, which may expose the data to the risk of theft, unauthorised copying or the like.[205]

In order to avoid any risk of unauthorised access once processing has ceased, the principle of storage limitation will be applicable as an obligation on data fiduciaries. Thus, data fiduciaries will only be able to retain personal data as long as it is required to satisfy the purpose for which it was collected. Thereafter, the said data may be anonymised or erased permanently to meet the requirements of the law. The key requirement is that once the object of processing has been achieved, the data, if retained, should not be capable of identifying any individual.[206]

The Committee is conscious that such a requirement may impose a compliance burden on fiduciaries in terms of a periodic review of all personal data retained by them. However, such review is necessary to make fiduciaries conscious of the personal data in their possession so that they can act, in a timely manner, to avoid any future breaches. The only exception to the principle of storage limitation would be instances where legal or sectoral or regulatory requirements may necessitate the storage of such personal data for further periods. For, instance the Know Your Customer Guidelines issued by the RBI require that information pertaining to the identification of the customer is to be retained for five years even after the closure of the account.[207] These must have overriding application.

Further, as long as the personal data is retained by the data fiduciary, it will be liable for all obligations that are imposed on it by the data protection law. The obligations will continue till the data has either been erased permanently or has been anonymised by the fiduciary. Therefore, obligations would continue to apply even after processing has ceased, as the data retained by the fiduciary remains capable of identifying individuals thereby qualifying as personal data.

---

[204] 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 on 1 May 2018).

[205] 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 on 1 May 2018).

[206] A key exception to this principle would however probably be processing for research purposes which has been discussed in Chapter 8.

[207] RBI, Master Direction – Know Your Customer (KYC) Direction, 2016 available at <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/18MDKYCD8E68EB13629A4A82BE8E06E606C57E57.PDF> (last accessed on 1 May 2018) at para 46.

VII. Data Quality

The principle of data quality implies that the personal data being used should be relevant to the purpose for which it is to be used and should be accurate, complete and kept up-to-date.[208] The requirements of accuracy, completeness and up-to-dateness are also linked to purpose and therefore should meet the requirements of the purpose for which the personal data was collected. Thus, in the case of studies that rely on longitudinal research, if the data does not meet the three requirements, then the processing of such data may not achieve the desired purpose and in fact may also lead to harm to the data principals.[209]

Accuracy, completeness and up-to-dateness of data are the key requirements of data quality. Personal data is intrinsically linked to individuals, who are therefore the most reliable source of data. The primary responsibility to provide accurate data to the data fiduciary will rest on the data principal. However, there is a corresponding obligation to ensure that data is complete, i.e. it will satisfy the purpose for which it was collected on the data fiduciary who is collecting such data.

In instances where personal data has been collected from parties other than the data principal, then the obligation would be on the data fiduciary to ensure accuracy, and in case of data being inaccurate, it is corrected, completed or updated upon request by the data principal. This is in conjunction with the right to correction, etc. which has been provided under our law to all data principals.[210]

Further, there will be a general obligation on the data fiduciary to ensure that the personal data being processed is accurate and to ensure that any onward disclosure or sharing of such data to third parties meets the requirements of accuracy. Where keeping the personal data up-to-date is necessary for the purpose of processing, such as in instances where the purpose relies on data remaining current, the fiduciary will be under a general obligation to take necessary steps to ensure that the data is kept up-to-date over time.[211]

VIII. Notification for Data Breach

(a) Need for Data Breach Notification

[208] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html> (last accessed on 1 May 2018).

[209] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013) available at <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html> (last accessed on 1 May 2018).

[210] This has been dealt with in Chapter 5 of this report.

[211] UK Information Commissioner's Office, Guidance on Data Quality available at <https://ico.org.uk/for-organisations/guide-to-data-protection/principle-4-accuracy/> (last accessed on 7 May 2018).

With large amounts of data being held by fiduciaries, the breach of personal data becomes a real possibility. A breach can have deleterious consequences for individuals whose personal data has been subject of the breach. Therefore, it becomes important to inform data principals about such instances so that they can take suitable measures to shield themselves from their harmful consequences. However, due to considerations of adverse publicity and avoidance of liability, fiduciaries may be dis-incentivised from reporting incidents of breach to individuals. Thus, a notification to the DPA upon the occurrence of a breach has been envisaged, in keeping with trends in other jurisdictions,[212] before a notification to the individual is made. It may be noted that such personal data breaches that are subject to obligations of notification should not be confused with breaches of data protection law generally.

(b) What constitutes a Personal Data Breach?

The definition of personal data breach will be structured in a manner that accounts for the three key principles of information security i.e. confidentiality, integrity and availability.[213] These principles offer the most holistic understanding of breach and comprehensively cover all the possible facets of a breach. Confidentiality breach implies an unauthorised or accidental disclosure of, or access to, personal data.[214] Integrity breach constitutes an unauthorized or accidental alteration of personal data.[215] An availability breach occurs when there is an accidental or unauthorised loss of access to, or destruction of, personal data.[216] A particular breach may however not fit neatly into any of these categories but may be combination of these. The significant elements of the definition of personal data breach would be the occurrence of 'disclosure' or 'access', 'alteration', and 'loss of access' or 'destruction' of personal data which occurs in manner that is either 'accidental' or 'unauthorised'.

It is also important to keep in mind that every security incident may not qualify as a personal data breach. Only security incidents that affect the confidentiality, integrity and availability of personal data, thereby compromising the data fiduciaries' ability to comply with the various requirements of data protection law will qualify as personal data breaches mandating notification.

---

[212] For example, Article 33(1), EU GDPR, Section 6, New Mexico Data Breach Notification Act, 2017.

[213] The fundamental principles of information privacy have been dealt in detail in our White Paper, see White Paper of the Committee of Experts on a Data Protection Framework for India available AT <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

[214] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

[215] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

[216] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 161.

(c) When does it need to be notified to the DPA?

A personal data breach may be of varying degrees of severity. For instance, an unauthorised hack of personal data held by a financial services company as well as the accidental deletion of contact details of members maintained by a social club, while both falling within the definition of personal data breach are not breaches of equal gravity. While the former, due to the possibility of significant harm to data principals, merits notification to the DPA the latter does not. In order to avoid the notification of relatively benign breaches of personal data, only such breaches will have to be notified that pose a likelihood of harm to the rights of data principals.

The Committee is cognisant that a notification requirement which depends on harmful consequences to the rights of the data principals may not afford sufficient clarity to fiduciaries. However due to the complicated nature of breaches it also not advisable to list specific thresholds in the law. It is therefore envisaged that the DPA will offer suitable guidance on what action is necessary to be taken.

The content of such notification should at the minimum include the nature of personal data that has been subject to breach and the number of individuals who have been affected by the breach, the possible consequences of the breach and the measures being taken to contain the breach.[217]

After becoming aware of such a breach, the fiduciary will be required to comply with the notification requirement as soon as possible. The obligation is being envisaged as a layered one where the fiduciary will be required to be in continuous communication with the DPA regarding the measures being taken to identify the scope and extent of the breach and the procedures being adopted to contain the breach. Though the obligation is to notify the DPA as soon as the circumstances surrounding the breach permit the fiduciary to do so, an outer limit for such notification should nonetheless be set so as to prevent risk of misuse.

(d) When does it need to be notified to individuals?

Upon notification, the DPA shall have the power to decide the severity of the breach and if relevant, the manner in which it needs to be reported to the individuals whose data has been breached. The breach should be notified to the individuals in instances where such a breach not only poses harm to the data principals, but also where some action is required on part of the principals to protect themselves from the consequences of the breach. The DPA has been granted the powers to determine when and how such notification is required to prevent the fiduciary from making a unilateral decision in this regard which may be motivated by factors other than best interests of the data principals. Further, the DPA is expected to better guide the actions of the data fiduciary and suggest or direct remedial measures, and it must be ensured that liability for the breach is suitably accorded in an adjudication action.

[217] Provisions on compensation may apply in such cases, see Chapter 9 of this report.

Failure to notify a breach would make the fiduciary liable to penalty under the provisions of the data protection law.

IX. Data Security

While the basis of a data protection law is the individual's right to informational privacy, obligations securing data protection need to be supplemented by implementation of security safeguards to ensure data security. According to the OECD principles[218] such security safeguards include physical measures, organisational measures (such as authority levels for accessing data) and informational measures (such as continuous threat monitoring).

The obligation to ensure data security is thus incorporated by the EU GDPR, which adopts the principles of information security requiring the integrity and confidentiality of personal data to be maintained at all times. Thus, personal data should be processed in a secure manner, ensuring that there is no unauthorised or unlawful processing and such data does not suffer from accidental loss or destruction.[219] Appropriate technical or organisational measures are required to be adopted to ensure data security.

Organisational measures include the application of information security policies in organisations handling data, business continuity plans in the event of breach, controlling access to data within the organisation etc.[220] Technical measures on the other hand include measures of physical and computer or information technology security. These would include adequate physical security of the premises, proper disposal systems for paper and e-waste etc.

Currently, in India the SPD Rules which have been issued under Section 43A of the IT Act[221] deal with data security. Rule 8 of the SPD Rules[222] defines reasonable security practices as implementation of security practices and standards, a comprehensively documented information security programme, and information security policies that contain managerial, technical, operational and physical security control measures commensurate with the information assets being protected and the nature of the business. The IS/ISO/IEC 27001 international standard is a recognised standard under the SPD Rules. Industry associations or entities which follow their own standards have to get them approved and notified by the Central Government.

---

[218] 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 on 1 May 2018).
[219] Article 5(1)(f), EU GDPR.
[220] UK Information Commissioner's Office, Guidance on Data Security, available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/security/> (last accessed on 07 May 2018).
[221] Section 43A, IT Act.
[222] Rule 8, SPD Rules.

With the introduction of a range of new rights and obligation under the data protection law however, the law will also have to re-emphasise the need for data security measures. The law will set out the general principle that fiduciaries in designing their security policies should ensure the confidentiality, integrity and accessibility of data at all times through organisational and technical measures keeping in mind the purpose and risk posed by their processing. The specificities of what security measures would meet the standards set by the law would be a sector-wise determination and require consultation between the DPA, sectoral regulators and industry bodies. These would be in conjunction with the organisational requirements that have been set out above.

Broader obligations of data security and organisational measures are intended to complement more specific obligations such as data minimisation, data quality, breach notification and storage limitation. Ultimately, the obligation of fair and reasonable processing will be overarching and underline and inform all other obligations. The Committee is of the view that the obligations which have been outlined above will ensure that processing of data occurs in a fair and reasonable manner. Further, they will ensure that any possibility of abuse in the envisaged fiduciary-principal relationship is mitigated, thereby upholding the best interest of the individual in a free and fair digital nation.

RECOMMENDATIONS

- The relationship between the "data subject" and the "data controller" is to be reformulated as a fiduciary relationship between the "data principal" and the "data fiduciary". **[Sections 3(13) and 3(14) of the Bill]**

- All processing of personal data by data fiduciaries must be fair and reasonable. **[Section 4 of the Bill]**

- The principles of collection and purpose limitation will apply on all data fiduciaries unless specifically exempted. **[Sections 5 and 6 of the Bill]**

- Processing of personal data using big data analytics where the purpose of the processing is not known at the time of its collection and cannot be reasonably communicated to the data principal can be undertaken only with explicit consent.

- A principle of transparency is incumbent on data fiduciaries from the time the data is collected to various points in the interim. Most prominently, a data fiduciary is obliged to provide notice to the data principal no later than at the time of the collection of her personal data. **[Sections 8 and 28 of the Bill]**

- There shall be obligations of data quality and storage limitation on data fiduciaries. However, the responsibility to ensure that the personal data provided is accurate will rest on the data principal. **[Sections 9 and 10 of the Bill]**

- There will be a provision of personal data breach notification to the DPA and in certain circumstances, to the data principal. **[Section 32 of the Bill]**

- Data security obligations will be applicable. **[Section 31 of the Bill]**

CHAPTER 5: DATA PRINCIPAL RIGHTS

In order to ensure a robust data protection law, it is essential to provide data principals with the means to enforce their rights against corresponding obligations of data fiduciaries. These rights are based on the principles of autonomy, self-determination, transparency and accountability so as to give individuals control over their data, which in turn is necessary for freedom in the digital economy. Specifically, some of these rights can be said to flow from the freedom of speech and expression and the right to receive information under Article 19(1)(a) and Article 21 of the Constitution.[223]

The Committee believes that a strong set of data principal rights is an essential component of an empowering data protection law. This chapter discusses the need, scope and implementation of three groups of rights as delineated in the White Paper. The first group consists of the rights to access, confirmation and correction; the second group consists of the rights of objection to processing, objection to direct marketing, objection to decisions made solely by automated processing, data portability and restriction of processing; and finally, the third group which deals with the standalone right to be forgotten.

A. Access, Confirmation and Correction

I. White Paper and Public Comments

The provisional views of the White Paper are that the right to seek confirmation, access and rectification should be incorporated in the data protection law.[224] However, the challenges in the implementation of these data principal rights, particularly relating to their expense and implementation, have been recognised. In this light, the White Paper suggests that a reasonable fee may be imposed by the organisations as determined by a DPA.[225]

---

[223] The freedom to know has been upheld in the cases of Reliance Petrochemicals Ltd v. Proprietors of Indian Express, AIR 1989 SC 190 at para 34; The State of U.P. v. Raj Narain, AIR 1975 SC 865 at para 74; S.P. Gupta v. Union of India, AIR 1982 SC 149 at para 66. The right to impart and receive information was discussed in The Secretary, Ministry of I&B v. Cricket Association of Bengal, AIR 1995 SC 1236 at para 124 (ii).

[224] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 127. The White Paper concludes that, "The right to seek confirmation, access and rectify personal data allow an individual control over data once such data has been collected by another entity. These rights may be suitably incorporated. However these rights are harder to enforce in the context of personal information that has been derived from the habits and observed behaviour of the individual and other such inferred insights. This information is nevertheless personal and an individual should be made aware of the fact that the data fiduciary has this sort of information."

[225] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 127. The White Paper concludes that, "Given that responding to individual participation rights can be costly for organisations, and comes with its set of technical challenges, a reasonable fee may be imposed on individuals when exercising these rights. This will also discourage frivolous and vexatious requests. The fees may be determined via sector specific subsidiary legislation or regulations. An illustration of this is the CIC Act under which the charge for accessing a copy of a person's credit information report by a specified user is laid down by the RBI via regulations."

Commenters have largely expressed support for the existence of the bundle of data principal rights discussed in the White Paper, namely the rights to confirmation, access and rectification. Several commenters have called for a wide scope for these rights, as the data belongs to the data principals and is being used by entities largely for commercial purposes. Some commenters have suggested that there should be an emphasis on ascertaining the identity of a requester.

Restrictions on scope have been sought by several commenters for interests such as public safety, law and order, sovereign function, privacy of other individuals, legal contraventions and cost. Other commenters have opined that data principals should not be refused access to data on the basis of grounds such as disproportionate effort, costs, volume of data, technical feasibility, inadequate manpower, frivolous claim, and alternate remedy. This is because it will enable data fiduciaries to refuse requests with ease, reduce individual control over data and de-legitimise the idea of a right. The imposition of a reasonable fee for exercise of these rights, as suggested in the White Paper, was widely supported. The exact fee, it was opined, could be determined by delegated legislation or sector-specific regulations. Some commenters were also against levying a fee, as it may discourage data principals from exercising their rights. Here the emphasis is on ensuring that there are no barriers to access data. It was suggested that a cost can be imposed only when requests are vexatious, frequent, unreasonable, or relate to older data.

A few commenters, however have expressed scepticism towards such rights *per se* as they believe that the Indian citizenry lacks awareness of these rights and due to the prospect of unwieldy implementation. However, most commenters supported the recognition of these rights as a necessary tool for the creation of a free and fair data protection framework.

II. Analysis

The right to confirmation refers to the right of a data principal to inquire regarding processing of her personal data by a data fiduciary. The right to access refers to the right of the data principal to gain access to her personal data which is stored with the data fiduciary. This right enables a data principal to gain access to a copy of all the personal data held about him/her by an entity.[226] The basis of these rights is to ensure that the data principal can understand, gauge and verify the lawfulness of processing.[227]

The rights to confirmation and access enable a data principal to enforce the substantive obligations of data fiduciaries. Only when a data principal knows what personal data a fiduciary has about herself and how it has been used, can she enforce her rights against the fiduciary. It is important to note that without the right to confirmation and access, the substantive obligations may become mere platitudes. Thus, in principle the rights to confirmation and access must find place in the law.

[226] Ian Long, Data Protection: The New Rules (Jordan Publishing, 2016) at p. 25.
[227] Recital 63, EU GDPR.

The scope of these rights must be guided by their rationale. These rights, as evident from the previous paragraph, are gateway rights that allow a data principal to understand the scope and extent of personal data that a fiduciary has. Consequently, these rights allow the data principal to take action, in case there is a breach of a substantive obligation by the fiduciary and are tools which a data principal can use to gauge the lawfulness of data handling by the data fiduciary. Keeping this in mind, the scope of the right to access and confirmation should be broad, and must include:

(i) All personal data relating to the data principal that has been collected by the data fiduciary;
(ii) The purposes for which the data fiduciary has collected such data;
(iii) The entities or persons to whom such data has been disclosed;
(iv) Information regarding cross-border transfer of such data;
(v) Information regarding the estimated duration for which data is stored, if feasible; and
(vi) Such other information regarding the collection, storage, handling and sharing of personal data that would have been provided under the obligation of notice that may need to be accessed again for transparent disclosure to the data principal.

It is to be recognised that the implementation of such an expansive right may be expensive.[228]

Further, there may be technical difficulties in complying with requests where large quantities of data are stored in an unstructured manner. After carefully analysing the opinion of commenters, the Committee is of the view that the expense involved in implementing such rights does not provide a principled reason to not have the right in the first place. It does however point to the need to take steps to ensure that these rights are made available by data fiduciaries. To do this, the Committee is of the opinion that a reasonable fee[229] may be charged by the data fiduciary for implementing the right to confirmation and access. Such fee, however, cannot be charged for purposes flowing from point (i) above, which relate to the personal data held by a data fiduciary and its purposes, which must be provided free to the data principal on request.

The DPA may be empowered to set time periods for complying with an access request. The RTI Act, which is akin to an access right only against public authorities, mandates a response in 30 days in the law.[230] However, it is our view that specifying a rigid deadline in a statute as a proxy for reasonableness, without a careful delineation of distinct types of data fiduciaries, the ease or onerousness of the obligations on them and the different types of personal data to

[228]Impact Assessment of Proposal for an EU Data Protection Regulation, Ministry of Justice (UK) (2012) available at <https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf> (last accessed on 19 April 2018) at p. 18.
[229] Supreme Court Rules, 2013, Third Schedule available at <http://www.supremecourtofindia.nic.in/sites/default/files/Supreme%20Court%20Rules,%202013.pdf> (last accessed on 11 May 2018) at p. 63.
[230] Section 7(1), RTI Act.

which access may be sought, may not be advisable. Thus, time periods must be set by delegated legislation. In case it is not feasible to comply within the time period that is set, the data fiduciary will be permitted an additional period to comply.

Data fiduciaries cannot refuse access to data principals on the basis of grounds such as disproportionate effort, costs, volume of data, technical feasibility, inadequate manpower, frivolous claims or any other alternate remedy. The only grounds for such refusal can be any relevant exemptions contained in this law, or any other law, or any other general conditions of refusal for any data principal right (such as, inadequate information regarding the identity of the data principal in the request for the right). Any other grounds for refusal would de-legitimise the idea of a right itself.

Further, the right to rectification (as mentioned in the White Paper) is being referred to as a right to correction in this report, where a data principal shall have the right to correct, complete or update any inaccurate or incomplete personal data about her. It empowers data principals to ensure accuracy of their personal data and may be a natural consequence of the right to access personal data, where such personal data is accessed and found to be inaccurate. The application of this right has a broad scope covering information about the data principal that a fiduciary possesses. It applies to both input personal data and output personal data. Input personal data refers to the data that the data principal provides to the data fiduciary whereas output personal data refers to the data that has been used to create a profile or reach a certain conclusion about an individual.[231]

It is important to maintain correct and up-to-date personal data in order to ensure the veracity of output decisions. This right is a necessary corollary to implementing the obligation to maintain accurate personal data, which is an obligation on data principals (during input) and data fiduciaries (thereafter). For example, if a data fiduciary analyses the social media activities of a data principal (such as the pages she likes, the videos she watches) and concludes that she likes a particular football club, the data principal will have the right to rectify this conclusion if it is incorrect.

The Committee is of the opinion that data fiduciaries should not be permitted to charge any fee for the implementation of the right to correction as it is the responsibility of the data fiduciary to ensure accuracy of personal data, when it holds such data. A reasonable period, specified by the DPA shall be given to fiduciaries to reflect the corrected data in their systems.

B. Rights to Objection, Restriction and Portability

[231] Article 29 Data Protection Working Party, Guidelines on Automated Individual decision-making and profiling for the purposes of regulation 2016/679 (adopted on 6 February 2018) at p. 24.

I. White Paper and Public Comments

The White Paper had some reservations in providing the right to object to processing since the right is only available when the data has been processed on the ground of public interest and legitimate interest (as under the EU GDPR), which may not be included as lawful grounds of processing in our framework.[232] However, the more specific right of objecting to processing for direct marketing was sought to be included within the data protection law, separate from the sector-specific regulations concerning direct marketing.[233]

On the right to not be subject to solely automated decisions, it was of the view that automated decisions may have adverse consequences, and to regulate them a practically enforceable right may be carved out.[234] The White Paper did not hold any provisional views on the right to restrict processing.

Finally, the White Paper concluded that data portability should be included as a right so as to empower data principals to give them control over their personal data. Therefore, the White Paper argued that individuals should be able to access and transfer the data that they have provided in a machine-readable format. Further, the provisional view taken was that all such data should be held in an interoperable format.[235]

A significant number of commenters have supported data principal rights, and corresponding provisional views discussed in this chapter. On the issue of the right to object, there was a mixed response. While some commenters agreed with the provisional view that the right to object would not be applicable in the Indian context, some others stated that it is an important right of data principals, which allows them to comprehend the uses of their personal data fully. Most responses however restricted their support of the right to object to that against direct marketing and against solely automated decisions. With regard to the right to object to processing for the purpose of direct marketing, a number of commenters have suggested a strictly consent based approach to direct marketing. Some of them have recommended an opt-out approach, and clear communication to data principals regarding their rights related to direct marketing (at the first stage of communication).

Additionally, a majority of commenters have cautioned against a blanket prohibition on automated decision making. Further, some commenters have stated that the right may only be

---

[232] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

[233] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

[234] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

[235] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 135.

applicable when the decision-making is purely through automated means, and the decisions can have potentially harmful or significant legal or economic effects (such as credit, housing, or employment opportunities) on the data principal. There is not much consensus on the applicability of this right where decision-making may have certain elements of human intervention. Some commenters have also generally highlighted the ambiguities and weaknesses of the right in the EU GDPR model.

While a number of commenters have supported a right to restrict processing, they have suggested variations or gradations in the application of this right. For instance, some commenters have advised that the right may only be applicable where personal data is inaccurate, where processing is being done for a commercial purpose, where there is some dispute regarding the legitimate grounds of processing, where the processing is unlawful and so on. On the other hand, some commenters have also argued against the incorporation of a right to restrict processing.

A majority of commenters have supported a right to data portability. However, a significant number of commenters cautioned against the heavy compliance burden on industry, as well as potential roadblocks in implementation. For example, processing a large number of requests for data portability may increase costs for the data fiduciary. In this scenario, a small fee could be charged from the data principal making such a request. Further, some commenters have suggested that it is imperative that data be stored in a standardised or universal machine-readable format. A few commenters have advised that standards related to data portability be developed by the industry.

II. Analysis

These rights represent a particular approach to ensuring lawfulness of processing — by vesting data principals with the power to hold the data fiduciary accountable. It is an extension of the core principle of autonomy, which this report commends as a key plinth of securing a free and fair digital nation. However as discussed previously in the report, autonomy is not absolute and may require to be curbed; not necessarily in favour of competing interests, but rather in the interest of more efficacious achievement of the ultimate public good of a free and fair digital economy. Implicit in such a framework is the need to not only be fair in principle, but fair in practice. This implies the use of the most efficacious method to ensure that processing is lawful and for the purposes for which consent was provided. Such method, may not always rest with the individual.

Keeping this in mind, the treatment of rights in this group can be divided into three sub-categories. First, the rights to object to processing, object to direct marketing and restriction of processing do not fit within the framework of lawful processing established by our framework. Regarding the right to object, in the EU GDPR such rights can be enforced by an individual owing to her particular situation, where the personal data is being processed lawfully under the grounds of public interest, exercise of official authority and legitimate interest. These grounds are not reflected in our framework in the same form as is envisaged

under the EU GDPR. Further, it may be difficult to provide for the specific grounds that would render such an objection valid. It is vague to provide a right to stop lawful processing on the basis of unenumerated grounds.

Finally, to the extent that processing is pursuant to a law or is in furtherance of a a non-consensual ground of processing, the onus of protecting the data will have shifted to the law which allows processing in each of these cases. For example, if Aadhaar data can be processed as per the Aadhaar Act by the Unique Identification Authority of India in order to maintain the integrity of the Central Identities Data Repository, processing must be as per the legal provision.[236] If individual circumstances change, then the individual will have a remedy if such change in circumstances renders future processing unlawful. Creating an overriding personal interest, without delineating it, appears ill-conceived.

Regarding the right to object to direct marketing, the Committee has come to the conclusion that data fiduciaries may only engage in direct marketing based on consent of the data principal, which is freely given as per the reinforced standards of our framework. Therefore, if the data principal does not consent to a request to be solicited by direct marketing, a data fiduciary may not be allowed to approach the data principal with marketing material on any mode of communication. This would do away with the need to have a separate right to object to direct marketing. It may be noted that while the TRAI captures a bulk of direct marketing activities that involve calls (via phones or mobiles) and text messages, direct marketing through emails or social media goes unchecked.[237] Therefore, addressing direct marketing through a consent-based framework would optimally fill this void and leave enough room for regulatory action in each sector.

Finally, the right to restrict processing may be unnecessary in India given that it is, in essence, a right given for availing of interim remedies against issues such as inaccuracy of data. Data principals can always approach the DPA or courts for a stay on processing in such cases, and the added benefit of exercising this right directly against a data fiduciary is not clear. Needless to say, the non-existence of this right, will not, in any way, derogate from the data principal's ability to withdraw consent for processing thereby rendering further processing unlawful.

The second group of rights relate to the right to object to automated decision-making and to access the logic behind it. In our view, these rights, again a response by the EU to emerging challenges from Big Data and AI, have a legitimate rationale. They are aimed at curbing harms due to prejudice and discrimination in output data owing to evaluative determinations without human review. The solution provided by this right is to simply involve a step of human review, which is not *per se* immune from prejudice. This is a change pertaining to the operational structure of an organisation. Such a change may be necessitated, provided it is carefully tailored to specific organisations and the nature of their processing activity. This, in

[236] Sections 23(2)(j) and 23(2)(l), Aadhaar Act.
[237] TRAI Telecom Commercial Communications Customer Preference Regulations, 2010, as amended, prohibit unsolicited commercial communications in the form of SMS and calls.

our view, is better achieved through an accountability framework which requires certain data fiduciaries, which may be making evaluative decisions through automated means, to set up processes that weed out discrimination. This is a constituent element of privacy by design which should be implemented by entities proactively, audited periodically and monitored by the DPA in case there are examples of unlawful processing. At the same time, such a model does not entirely denude the individual of agency. If discrimination has ensued as a result of *per se* lawful, yet discriminatory automated processing, individuals are always at liberty to go to courts for breach of fiduciary duties. Thus, the interests underlying such rights, can be more efficaciously achieved by an *ex ante* accountability model.

Third, the right to data portability is critical in making the digital economy seamless. This right allows data principals to obtain and transfer their personal data stored with a data fiduciary for the data principal's own uses, in a structured, commonly used and machine-readable format. Thereby, it empowers data principals by giving them greater control over their personal data. Further, the free flow of data is facilitated easing transfer from one data fiduciary to another. This in turn improves competition between fiduciaries who are engaged in the same industry and therefore, has potential to increase consumer welfare.[238] As the right extends to receiving personal data generated in the course of provision of services or the use of goods as well as profiles created on the data principal, it is possible that access to such information could reveal trade secrets of the data fiduciary. To the extent that it is possible to provide such data or profiles without revealing the relevant secrets, the right must still be guaranteed. However, if it is impossible to provide certain information without revealing the secrets, the request may be denied. The right to transfer or transmit data from one fiduciary to the other should however be limited by constraints of technical feasibility. That is, data fiduciaries would not be obligated to provide data portability if they are able to prove that technical capabilities as currently existing would make the required access or transfer unfeasible.[239] The market standards of technical feasibility of transference of data may be set through codes of practice developed by the DPA to ensure that fiduciaries do not use this reasoning to deny data principals the right to portability. Further, to address concerns of costs, fiduciaries may be allowed to charge a reasonable fee to effectuate this right. In our view, such a balance captures the principled significance of the right while remaining cognisant of the practical difficulties in its implementation today.

C. The Right to be Forgotten

The right to be forgotten refers to the ability of individuals to limit, de-link, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic.[240] Such disclosure, may or may not be a consequence of unlawful processing by the data fiduciary. This is because, the right flows from the general obligation

[238] Paul de Hert et al., The right to data portability in the GDPR: Towards user-centric interoperability of digital services, Computer Law & Security Review (2017) at p. 9.
[239] Article 29 Data Protection Working Party Guidelines on the Right to Data Portability available at <http://ec.europa.eu/newsroom/document.cfm?doc_id=44099> (last accessed on 20 April 2018).
[240] Michael J. Kelly and David Satola, The Right to be Forgotten, University of Illinois Law Review (2017) at p. 1.

of data fiduciaries to not only process lawfully, but also in a manner that is fair and reasonable. In this context, it is essential to take into account a data principal's understanding of unfairness. Therefore, if she believes certain processing to have unfairly disclosed personal data, then she should be able to have a remedy against such disclosure. The right to be forgotten therefore provides a data principal the right against the disclosure of her data when the processing of her personal data has become unlawful or unwanted.[241]

Implicit in this formulation is the fact that the right itself is defeasible. There is no principled reason as to why the data principal's assessment of unfairness would override that of the fiduciary. Where a disclosure has taken place on the basis of the consent of a data principal, it would be appropriate that the unilateral withdrawal of such consent could trigger the right to be forgotten. In other cases where there is a conflict of assessment as to whether the purpose of the disclosure has been served or whether it is no longer necessary, a balancing test that the interest in discontinuing the disclosure outweighs the interest in continuing with it, must be carried out.

In carrying out this balancing test, certain principled and practical issues must be considered: first, in case of a direct or subsequent public disclosure of personal data, the spread of information may become very difficult to prevent;[242] second, the restriction of disclosure immediately affects the right to free speech and expression. The purpose for a publication may often involve matters of public interest and whether the publication is 'necessary' may depend on the extent of such public interest. The appropriateness of a right to be forgotten in these circumstances would require that the right to privacy be balanced with the freedom of speech.[243]

I. White Paper and Public Comments

In the White Paper, it was tentatively proposed that the right to be forgotten should be incorporated in the data protection law.[244] However, this right must be granted after a careful balancing of the right to freedom of speech and expression with the right to privacy. The

[241] House of Commons, Justice Committee, The Committee's opinion on the European Union Data Protection framework proposals: Volume I, HC 572, (1 November 2012) at p. 26, quoting a former Deputy Information Commissioner of the UK as saying, in relation with an earlier draft of the EU GDPR: "When you unpick it, much of what is there of the right to be forgotten is just a restatement of existing provisions—data shan't be kept for longer than is necessary; if it has been processed in breach of the legal requirements it should be deleted, which goes without saying."

[242] House of Lords, European Union Committee, EU Data Protection law: a 'right to be forgotten'? HL 40 (30 July 2014), the Committee criticised the Google Spain judgment, finding that "Once information is lawfully in the public domain it is impossible to compel its removal, and very little can be done to prevent it spreading. … A judgment which cannot be complied with brings the law into disrepute."

[243] Thus, in Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01, the Court of Justice of the EU found that restrictions on the publication of personal data would require national courts and national legislatures to balance the same against rights such as the freedom of expression. Other considerations may also be relevant. Some Indian courts have grounded this right in the concept of reputation and morality, rather than privacy. In Vasunathan v. The Registrar General, High Court of Karnataka, 2017 SCC Karnataka 424, the Court held that while the certified copy of the order may contain the name of the petitioner's daughter, internet search engines will not be permitted to index in sensitive cases involving women in general as it may cause loss of reputation in society.

[244] The Supreme Court had also adverted to such a right. Per *Puttaswamy*, (2017) 10 SCALE 1, at p. 33.

White Paper was of the preliminary view that the data fiduciary should carry out this balancing test on the basis of clear parameters.[245]

There was a division of opinion in public responses on this issue. Some commenters were of the opinion that the right to be forgotten should not be incorporated into India's data protection framework as there is no additional benefit to be gained by guaranteeing this right to individuals. Further, it was argued that incorporating a right to be forgotten would have a detrimental impact on individuals' ability to access information on the internet. Therefore, there is an obvious conflict between balancing this right and other rights such as that of free speech. Alternatively, some commenters believed that the right to be forgotten should be incorporated into India's data protection framework. On the scope of the right, commenters were of the opinion that it should not include the right to erase 'public information' about an individual. Some commenters also agreed that any 'derivatives' of personal data, or data which has been processed by an organisations' algorithms should not be within the scope of this right. Other commenters also argued that certain types of information, such as credit information, criminal history, court orders and so on, should not be permitted to be deleted as they are required in greater public interest, or in interest of law enforcement, or for the purpose of monitoring illegal or fraudulent activities.

On the issue of which entity should carry out the balancing test, some commenters believed that relying on data fiduciaries to make this decision will be excessively burdensome; there is a chance that they will act in their own interest and there will be considerable divergence in practice. Therefore, these commenters suggested that the data protection law should contain specific guidelines, which can be used by data fiduciaries to make their decisions.

II. Analysis

The right to be forgotten is an idea that attempts to instil the limitations of memory into an otherwise limitless digital sphere. A limited memory and the consequent need to both remember and forget are essential facets of the human condition. The internet, with its currently vast reserves of data storage appears to facilitate timeless memory. As a result, the ability to forget is seriously denuded. This might not be entirely undesirable— collective attempts at forgetting have often involved attempts at rewriting history.[246]

However, the individual desire to forget is an expression of autonomy that may be worthy of protection. This is especially the case, if we accept that data flows are initiated by the individual who must be free and to whom others must be fair. But in considering such a right, it is imperative to note that other individual freedoms and collective goods may be impacted. Removing publicly available information takes away from an individual's right to know; at

[245] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 18 April 2018) at p. 141.

[246] Howard Zinn, A People's History of the United States (Harper Perennial Modern Classics, 2015). For almost two centuries people were told that Columbus was a great hero whereas Howard Zinn's research illuminated how Columbus may actually have been guilty of genocide, torture, rape, enslavement, and thievery.

the same time, it abridges the freedom of the press which has published the story in the first place. Further, if every individual started exercising a right to be forgotten over various types of personal data, the nature of the public realm of information itself would be brought into question as such information may be permanently deleted. Of particular concern is the risk that the deletion may be not just from the public space but also from private storage, preventing later publication as well. Therefore, in order to address these free speech concerns, there may be a need to make a distinction between restrictions on disclosure (such as de-linking in search results) and permanent erasure from storage, which may not be permitted as a separate individual participation right. Further, any implementation of this limited right to be forgotten must involve a careful consideration of the following principled and practical issues:

(a) Balancing the Right with Competing Rights and Interests

The first issue that arises is that the core of the right to be forgotten, i.e. deletion of disclosed or published information, interferes with someone else's right to free speech and expression as well as their right to receive information.[247] Further, a broad based right to be forgotten may be susceptible to misuse.[248] As discussed above, the Committee is of the view that permanent deletion of personal data from storage should not be a part of this right. While determining whether to allow for the right to be forgotten, the appropriateness of consequent restrictions on the right of free speech and expression and the right to information would necessarily have to be considered.[249] This should, however, be constrained through the insertion of a statutory balancing test. Such balance may be achieved through the application of a test with five criteria:[250]

(i) the sensitivity of the personal data sought to be restricted.
(ii) the scale of disclosure or degree of accessibility sought to be restricted.[251]
(iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office).
(iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public).

[247] This has been raised as a matter of considerable concern, with one scholar even referring to the right as 'the biggest threat to free speech on the Internet in the coming decade.' See, Jeffrey Rosen, The Right to Be Forgotten, 64 Stanford Law Review Online (2012) at p.88.
[248] Muge Faz, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, 3 International Data Privacy Law 3 (August 2013) available at https://academic.oup.com/idpl/article/3/3/149/622037 (last accessed on 2 June 2018).
[249] Mr X v. Hospital Z, 1998 (8) SCC 296. In this case, there was a conflict between the right to privacy of one person and the right to a healthy life of another person. The Court held that, in such situations, the right that would advance public interest would take precedence.
[250] These criteria constitute a slight modification of the criteria developed in Google's internal policy. See, Luciano Floridi et al, Report of the Advisory Council to Google on the Right to Be Forgotten (February 2015) p. 7-14 available at <https://static.googleusercontent.com/media/archive.google.com/en//advisorycouncil/advisement/advisory-report.pdf> (last accessed on 1 May 2018).
[251] Significantly, in Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01, it was found that the exemption for "personal or household activity" would not apply if the information is "made available to an indefinite number of persons." The criterion suggested views this question of availability as a question of degree.

(v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation).

Since we live in a dynamic digital age, there may be certain situations wherein the information in question (against which a right to be forgotten order was passed) has subsequently become relevant to the public again. Therefore, the law may need to have provisions for the review of such decisions.[252]

(b) Appropriate Entity for the Approval of Requests

Considering that the right to be forgotten hinges on the aforementioned balancing test, it is critical to assign this test to an appropriate entity. In the EU, following the recognition of the right to be forgotten, companies like Google received large volumes of requests from individuals for de-listing. EU law envisages that the data fiduciary would have to consider the requests and apply the balancing test mentioned above. In effect, this amounts to the privatisation of regulation and shifts responsibility for the protection of fundamental rights to private entities that are not constrained by democratic accountability. Given that a rejection of de-listing could involve legal consequences for the fiduciary, there may also be considerable incentive to not reject requests, especially when they are in high volume and when the controller does not have the resources to regularly carry out legal assessments. This position of the law in the EU has been criticised on this ground.[253]

Further, 'notice and takedown' procedures in India (for defamatory and obscene content, for instance) has been seen to be problematic as they appeared to require intermediaries to become private censors determining free speech rights.[254] Further, the Supreme Court held in 2015 that under the IT Act, intermediaries should only be required to take down content where they have been notified of objectionable content by the government or through a court order.[255]

Balancing the right to privacy and other individual interests with the freedom of speech and expression is a core public function. The Supreme Court of India, when faced with a question of competing rights, has laid down a well-established test on how to adjudicate such a question on its merits.[256] In India, this balancing function is most appropriately seen as an

---

[252] Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, The Centre for Internet and Society (2011) available at <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf> (last accessed on 20 April 2018). It suggests a 'put-back' procedure in the context of takedown under the IT Act.

[253] Michael J Kelly and David Satola, The Right to be Forgotten, University of Illinois Law Review (2017) at p. 16.

[254] Rishabh Dara, Intermediary Liability in India: Chilling Effects on Free Expression on the Internet, The Centre for Internet & Society (2011) available at <https://cis-india.org/internet-governance/intermediary-liability-in-india.pdf> (last accessed on 20 April 2018).

[255] Shreya Singhal v. Union of India, (2015) 5 SCC 1 at para 122.

[256] Mr. X v. Hospital Z, 1998 (8) SCC 296.

adjudicatory one. Thus, right to be forgotten requests, in keeping with the scheme of our framework, should be made to the Adjudication Wing of the DPA (as discussed further in Chapter 9).

(c) Breadth of Application of Orders

When a determination has been reached as to the fiduciary's obligation to delete the disclosure of personal data, it becomes essential to ascertain what the breadth of the order is. Where data has been made public, there is every possibility that it has been replicated and published further on other webpages. The EU GDPR provides that a data fiduciary (controller in its language) who has been obliged to delete the disclosure of data should inform other fiduciaries of the data principals' request for deletion. Given that the Committee envisages the right to be one that is granted by the Adjudication Wing of the DPA, whether to impose such obligation or not may be left to the discretion of the relevant Adjudicating Officer and its statutory mandate of narrowly tailoring the exercise of the right. It may be inappropriate to automatically apply orders to other fiduciaries not specifically named in the data principal's request because the approval of a request may have been made on the basis of the nature of the named fiduciary.

RECOMMENDATIONS

- The right to confirmation, access and correction should be included in the data protection law. **[Sections 24 and 25 of the Bill]**

- The right to data portability, subject to limited exceptions, should be included in the law. **[Section 26 of the Bill]**

- The right to object to processing; right to object to direct marketing, right to object to decisions based on solely automated processing, and the right to restrict processing need not be provided in the law for the reasons set out in the report.

- The right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability on the basis of the five-point criteria as follows:

    (i) the sensitivity of the personal data sought to be restricted;
    (ii) the scale of disclosure or degree of accessibility sought to be restricted;
    (iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office);
    (iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public); and
    (v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation). **[Section 27 of the Bill]**

- The right to be forgotten shall not be available when the Adjudication Wing of the DPA determines upon conducting the balancing test that the interest of the data principal in limiting the disclosure of her personal data does not override the right to freedom of speech and expression as well as the right to information of any other citizen. **[Section 27 of the Bill]**

- Time-period for implementing such rights by a data fiduciary, as applicable, shall be specified by the DPA. **[Section 28 of the Bill]**

CHAPTER 6: TRANSFER OF PERSONAL DATA OUTSIDE INDIA

The last two decades have seen an explosive expansion of the internet and the number of internet users across countries. However, what is more significant is that the private nature of internet service providers and the free flow of their services has resulted in the globalisation of the internet as well,[257] such that information produced in one country is easily accessible in another. The flow of data remains an imperative for a healthy digital economy. However, a data protection regime that assures individuals of certain rights must ensure that such data flows are not indiscriminate, and that a reasonable level of protection is accorded to such data irrespective of where it is transferred to.

Apart from the legal conditions permitting the flow of personal data across borders, an increasingly relevant method for making jurisdiction effective is to place requirements relating to the storage and processing of personal data within the territory of a state. A policy of storage and processing of personal data within the territorial jurisdiction of a country is advocated to ensure effective enforcement and to secure the critical interests of the nation state. However, due to the substantial costs involved in setting up digital infrastructure to store data locally and in the interests of a free digital economy, the ramifications of such a policy need to be carefully considered. This chapter discusses cross-border flows of personal data as well as requirements for the storage and processing of such data within the territorial reach of a country, outlining the approach of the Committee on these points.

A. White Paper and Public Comments

On the question of when personal data may be transferred abroad, the White Paper identified two preconditions of adequacy and comparable level of protection for such data.[258] The provisional view taken was that the adequacy test, which requires the DPA to determine whether a country possessed adequate level of protection for personal data, was beneficial since it ensured a smooth two-way flow of personal data critical for a digital economy.[259] In the absence of such a certification, the data fiduciary would bear the responsibility of ensuring that personal data, once transferred would continue to enjoy the same level of protection as in India.[260]

A majority of commenters suggested that the adequacy test, that requires the DPA to determine if data protection laws in the transferee jurisdiction are adequate (utilised by the EU GDPR in regulating the cross-border flow of data), may be adopted. Interoperability,

[257] Orin S. Kerr, The Fourth Amendment and the Global Internet, 67 Stanford Law Review (2015).
[258] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.
[259] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.
[260] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 68.

greater leverage to access markets and effective protection of citizens' data were key rationales. On the other hand, commenters who argued against the adequacy test reasoned that the determinations were an expensive, time consuming and restrictive process since most countries in the world were yet to adopt laws on data protection. Instead, the principle of accountability was suggested which makes the transferor entity responsible for data protection, where the data crosses borders.[261]

With respect to data localisation, the White Paper recognised the need for treating different types of personal data differently and a one-size-fits-all model was not considered appropriate.[262] It was felt that India would have to carefully balance possible enforcement benefits of localisation with the costs involved in mandating such a policy in law.

Commenters were largely unanimous in rejecting a homogenous framework and stressed on the need for sector specific measures along with discretion for a case-by-case determination. However, a majority of the commenters, including major technology companies and industry groups took a view against mandatory data localisation on the basis that such a move may have an adverse impact on the industry. Some commenters supported mandatory localisation of personal data for reasons of law enforcement, preventing foreign surveillance, creating local jobs, ensuring jurisdiction of Indian authorities over data breaches and strengthening of the Indian economy.

B. Analysis

I. Cross-Border Transfer of Personal Data

It is essential to ensure that the interests of effective enforcement of the law, economic benefits to Indians need to be core to any proposed framework for cross-border transfer. However these must not unjustifiably impede international flow of personal data, which itself is beneficial in many ways for Indians. This is similar to the physical economy in India where a combination of free movement of goods and transfer restrictions operate alongside each other. The key questions are where and how the line can be drawn in determining which data can be transferred across borders.

One might wonder why the aforementioned formulation inverts what is perceived to be the status quo, where freedom to transfer is the rule and restrictions on such freedom are the exception. It is only partially accurate to describe the status quo as such. In its operation, the freedom to share personal data in the digital economy operates selectively in the interest of certain countries that have been early movers. For example, the US can, without any detriment to its national interest, support a completely open digital economy by virtue of its technological advancement. The need for local enforcement is also largely accounted for

[261] Comments in response to the White Paper submitted by Cody Ankeny on 30 January 2018, available on file with the Committee.

[262] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 75.

owing to the personal jurisdiction that the US exercises over a large number of technology companies as well as the large volumes of data stored in its territory.[263] Thus, any advocacy of complete freedom of transfer of personal data in the digital economy, must perhaps be viewed cautiously.

On the other hand, in the EU, the operation of prescriptive rules restricts the permissibility of cross-border transfers to a limited set of circumstances. These include transfers to jurisdictions where data protection norms are deemed 'adequate', transfers that are subject to approved contractual clauses or rules, or other prescribed circumstances where the need for transfer is seen to be substantial or the risk of harm is reduced.[264] Only 12 countries have received adequacy certification from the EU,[265] with data sharing with the US being limited to the privacy shield framework.[266] Bilateral agreements have been entered into with the US, Australia and Canada for sharing of airline passenger data for law enforcement.[267] Most data sharing to countries other than those that have been deemed 'adequate' therefore appears to happen at the level of companies who enter into contracts with standard clauses or through binding corporate rules.

The European Commission has so far issued two sets of standard contractual clauses, first for transfers from data controllers to other data controllers and second for transfer to processors, outside the EU/EEA.[268] The contractual clauses, however, have been criticised for not being implementable due to the difficulty faced by DPAs in identifying non-compliance.[269] Further, the very validity of standard contractual clauses has been referred to the Court of Justice of the EU, thereby making the future of such transfers uncertain.[270] The binding corporate rules

[263] A 2013 report by McKinsey estimated that the US is home to one-third of the world's data. This translated to 898 exabytes of data (1 exabyte = 1 billion gigabytes). See Game changers: Five opportunities for US growth and renewal, McKinsey Global Institute (July 2013) available at <https://www.mckinsey.com/featured-insights/americas/us-game-changers> (last accessed on 23 April 2018).

[264] See Chapter 5, EU GDPR.

[265] These include Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay. See Adequacy of the protection of personal data in non-EU countries available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en> (last accessed on 21 April 2018).

[266] The EU-US privacy shield decision was adopted on 12 July 2016 and the privacy shield framework became operational on 1 August 2016. The framework protects the fundamental rights in case of data transfer from the EU to the US for commercial purposes. See EU-US Privacy Shield available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> (last accessed on 21 April 2018).

[267] Transfer of air passenger name record data and terrorist finance tracking programme available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/transfer-air-passenger-name-record-data-and-terrorist-finance-tracking-programme_en> (last accessed on 21 April 2018).

[268] See Model contracts for the transfer of personal data to third countries available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en> (last accessed on 21 April 2018).

[269] See A. Zinser, The European Commission Decision on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries: an Effective Solution?, 3(1) Chicago-Kent Journal of Intellectual Property, (2003).

[270] Clyde & Co, Irish High Court refers validity of model contract clauses to ECJ, Lexology (31 October 2017) available at <https://www.lexology.com/library/detail.aspx?g=ce3c1970-4382-40df-8de0-3e99ff571d27> (last accessed on 21 April 2018). The first referral order in The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2016 No. 4809 P.) available at

on the other hand only provide a framework for the transfer of data within multinational companies, with the rules requiring approval not only from the DPA appointed as the lead authority for this purpose but also from the DPAs of other EU countries from where the data is being transferred outside the EU.[271]

The discussion above must inform the alternatives that we may consider regarding the permissibility of cross-border transfers of personal data but to understand where we must draw the line, it is imperative to keep in mind India's interests in regulating such transfers. The starting point in this context must be an assessment of the types of personal data to which the law applies. This is the universal set of personal data to which rules relating to cross-border transfers can be applied since (for reasons explained in Chapter 2 on jurisdiction) India's territorial and passive personality interests are impacted. As this is the scope of the law itself, any cross-border flow of other types of data would not be barred by this law. Needless to say, distinct concerns may regulate such activity and the Government may frame a suitable policy in this regard, but such analysis is beyond the remit of our Committee.

Personal data that is maintained in India will always have the protection of India's data protection regime. However, national interest would require that at least an adequate level of protection should be accorded to personal data transferred abroad. Given the mobility and seamless transferability of data, a failure to impose such a restriction would seriously compromise the efficacy of the substantive protections the law provides. It is thus necessary that rules ensuring such adequate protection be implemented.

The question that next arises is how such protection is to be effectuated. It follows from our discussion of the limited nature of adequacy determinations in the EU framework that any analogous model primarily based on such determinations should be looked at cautiously. Though it has significant merits in terms of providing certainty to entities desirous of transferring data, making it the primary method of transfer puts undue enforcement burden on regulators. Whether the DPA in India will have the capacity to do this is an open question, though for a new entity possessing such capacity on Day One is unlikely. Rather, the alternative mode of approved contractual clauses or rules must be improved upon, especially by ensuring that they are in a form that provides adequate protection and are better capable of being enforced.

<https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf> (last accessed on 24 April 2018). It is noteworthy to point that in the course of the ongoing Schrems litigation with respect to standard contractual clauses, the Irish High Court has issued a second referral order to the Court of Justice of the EU which questions the validity of the entire EU-US privacy shield itself. See Privacy Shield now facing questions via legal challenge to Facebook data flows (13 April 2018) available at <https://techcrunch.com/2018/04/13/privacy-shield-now-facing-questions-via-legal-challenge-to-facebook-data-flows/> (last accessed on 21 April 2018); The second referral order in the case of The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2016 No. 4809 P.) available at <https://www.documentcloud.org/documents/4436535-Ref.html> (last accessed on 21 April 2018).

[271] Under the mutual recognition procedure to which 21 EU countries are part of, once the lead authority has concluded that the rules meet all requirements as per law, the other authorities treat the lead authorities' opinion as sufficient basis to issue their own national permits. See Binding Corporate Rules available at <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_en> (last accessed on 21 April 2018).

It is our view that the interest of a free and fair digital economy will best be served by a framework where a model contract for such transfers is formulated by the DPA. Entities transferring data would be mandated to incorporate such model clauses in the relevant contracts.[272] The model contract will contain the key obligations on transferee entities as per the Indian law. These include security, purpose limitation, storage limitation and a responsibility to fulfil rights of individuals. Further, the transferor entity who is bound by the Indian law will undertake to bear liability for any breach by the transferee in relation to the aforementioned obligations. A self-certification by such entity that the contract is in line with the model contract, and that it undertakes to bear liability as mentioned above, will be recorded. These records will be subject to compulsory audit and periodic reporting to the DPA. A similar set of binding corporate rules which may be termed as 'intra-group schemes' can be adopted by group companies for *inter se* transfer of data within the group.

Such entity-led transfers should be the primary method for ensuring equivalent protection for Indian personal data abroad. However, despite the practical difficulties of entering into adequacy assessments, the role of the sovereign in green-lighting certain countries for permissibility of transfer cannot be entirely discounted. This is because, if the very rationale of this law is to protect data of Indians, such rationale will be defeated if data can be transferred abroad without the possibility of any regulatory preconditions being set. The option must be given to the Government of India, in consultation with the DPA to enter such determinations of countries where personal data can be transferred freely. By continuing this option, the law provides a lever for adequacy assessments, contingent on capacity developing over time, reducing transaction costs for entities. However, the law is not contingent on a positive adequacy determination for transfer thereby leaving entities the autonomy to transfer data on the basis of standard contracts. In our view, this is a harmonious balance.

In addition, we may mention that transfers of personal data on the basis of consent have to be permitted. Despite the difficulties this might raise in terms of enforcement, provision for such transfer may be necessary to respect the autonomy of the data principal. For the purposes of sensitive personal data, the consent would have to be explicit (as discussed in Chapter 3). There would however be another exemption to the operation of the regime for the transfer of personal data outside India. There may be a set of hitherto unknown situations where data that is processed must necessarily be transferred abroad without restriction. This may be for practical reasons, e.g. emergencies or strategic ones, or the need to bolster bilateral trade. Since this is best assessed by the executive, the Central Government should have the power to determine such instances on a case by case basis and exempt it from any restrictions (described below) which may apply.

[272] For group companies, *inter se* transfers should be permitted based on a standard template that will be pre-approved by the DPA. There will be no need for regular reporting to the DPA every time a contract is entered into or a transfer is made.

II. Exceptions to Free Transfer of Personal Data Outside India

Conditions regarding the permissibility of cross-border transfer of personal data would certainly ensure that data is not deprived of all protection abroad, but it is not enough in and of itself. Despite the conditions discussed above, the imperative of cross-border flow of personal data may have to be balanced with India's interests in enforcing its data protection law in a successful manner. Effective enforcement will invariably require data to be locally stored within the territory of India and this would mean that such a requirement, where applicable, would limit the permissibility of cross-border transfers as outlined above. Different jurisdictions have followed varying practices in this regard. Whereas China localises internet-based mapping services, critical information infrastructure and banking data,[273] Canada localises public interest data held by government agencies, schools and hospitals,[274] Australia localises health data[275] and so on. In certain cases, such as in jurisdictions like China and Russia, the data that is localised is not permitted to be transferred outside territorial borders.[276] In other countries such as Vietnam, a copy of the data is kept on a local server, but data transfer outside the jurisdiction is also permitted.[277]

Though there is no exact alignment on the categories of data subject to such rules, the rationale is clear: any personal information deemed critical in national interest or for heightened privacy protection is localised. Such rules go beyond the regulation of transfer and take steps towards curtailing flow more strictly. The range of strict restrictions described above appear to be towards one end of the spectrum of barriers that may be placed on the free flow of personal data; this may be compared with the position in the US where there are minimal restrictions as has been discussed in the preceding section of this Chapter.

For the purposes of India, it is the Committee's belief that neither of the above extremes need be the appropriate path. Any obligation requiring the storage and processing of personal data within India should be based on clear advantages arising out of the implementation of such a measure. A policy preventing copies of personal data from being transferred abroad could take two forms: first, a mere requirement to maintain one live, serving copy of personal data (while allowing other copies to be transferred), or second, a stricter requirement that personal data be processed only within India. Both these policies would align with several interests for India, including effective enforcement of the Indian law, promotion of growth in the Indian

[273] Article 31, Cyber Security Law of China provides a non-exhaustive list of selected critical industries and areas whose information infrastructure would be regarded as 'critical information infrastructure'. It includes public communications, information services, energy, transport, water conservancy, finance, public services, and e-governance etc., and more broadly, other information infrastructure, which may cause serious consequences if it suffers any damage, loss of function, or leakage of data. An unofficial English translation of this legislation is available at: The National People's Congress of the People's Republic of China, People's Republic of China Network Security Law (2016) available at <http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm> (last accessed on 8 April 2018).

[274] Asia Pacific Economic Cooperation, Cross Border Privacy Rules System. There are currently five participant countries, namely US, Mexico, Japan, Canada and the Republic of Korea.

[275] Section 77, Personally Controlled Electronic Health Records Act, 2012.

[276] See Article 16(4)(7), Federal Law No. 242-FZ (Russia); Article 37, Cyber Security Law of China.

[277] Decree on the management, provision and use of Internet services and online information (No. 72/2013/NDCP) (Vietnam).

digital ecosystem and avoidance of vulnerabilities in our fibre optic cable network system. Such benefits have been listed in detail below.

(a) Benefits

(i) Enforcement

The question of local storage of personal data is intrinsically connected to the enforcement of domestic law generally and in particular, the data protection law itself. Intelligence agencies and law enforcement bodies have an increasingly challenging role in the 21st century. They must check the growth of terrorism, prevent cyber-attacks and tackle cyber-crime. Investigation of ordinary crime too often requires access to personal data. Further, the obligations on data fiduciaries pursuant to the data protection framework themselves require effective enforcement by the DPA.

In order to fulfil this mandate, law enforcement bodies often need to gain access to information that is held and controlled by data fiduciaries.[278] As a result of this, it is important for the law to acknowledge the importance of quick and easy access to information to effectively secure national security and public safety. A requirement to store personal data locally would boost law enforcement efforts to access information required for the detection of crime as well as in gathering evidence for prosecution. This is because it is easier for law enforcement agencies to access information within their jurisdiction as compared to awaiting responses to requests made to foreign entities which store data abroad. However, it is advisable that in the future, nation states should strive towards harmonisation to create an enforcement regime that provides for effective information sharing.

In academic writing, reservations have been expressed against this argument.[279] Three claims are made in this regard: first, domestic enforcement may not be hampered by non-availability of data since many laws require cloud service providers to share access with law enforcement agencies; second, business may be driven away because processing data locally would be costly; third, the law may not be followed because controllers ('fiduciaries' in our understanding) would know that the law will be difficult to enforce. It is necessary to consider these arguments carefully.

First, while there may be some degree of compliance with laws having extra-territorial operation, in practice, the enforcement of any order actually made under such laws may be both difficult and time-consuming.[280] For non-complying entities outside a particular

[278] Tatevik Sargsyan, Data Localisation and the Role of Infrastructure for Surveillance, Privacy, and Security, 10 International Journal of Communication (2016).
[279] Anupam Chander and Uyên P. Lê , Data Nationalism, 64 Emory Law Journal (2015).
[280] For instance, it has been pointed out that exercising jurisdiction under a law is only one part of the exercise and an authority's intervention could be "rendered futile if its orders against defendants outside its jurisdiction cannot be enforced", see Justice S. Muralidhar, Jurisdictional issues in Cyberspace, 6 The Indian Journal of Law and Technology (2010) at p. 33.

jurisdiction, the enforcing country would be required to issue an MLAT request[281] to the country enjoying personal jurisdiction over the entity. The MLAT process is well documented to be deeply flawed and overly time-consuming and therefore recourse to such a regime may not be the ideal enforcement solution unless adequate improvements are effected in the future.[282]

Second, any argument highlighting the costs arising from the domestic retention of personal data must meet a higher burden. All or most legal obligations give rise to economic costs for regulated entities and thus mere increase in costs cannot be reason not to introduce legal change. Rather, it must be shown that the costs incurred due to rules demanding local processing outweigh the benefits of such a requirement. This must be done while keeping in mind that the benefits run to the core objectives of data protection. While some commenters have suggested that mandating storage and processing locally may have significant financial implications, the real question is whether the actual costs of local processing will be such that it overrides the benefits of companies having access to the burgeoning consumer database in India.[283] There is no evidence presented before us that demonstrates the results of this cost-benefit analysis conclusively.

Third, that the law will not be enforced is not an adequate justification. For instance, while the enforcement status of similar laws in Russia and China are unclear, the enforceability of any such rules would depend on local enforcement capacity and prioritisation. This argument puts the cart before the horse.

It is important to note that currently, eight of the top 10 most accessed websites by individuals in India are owned by US entities.[284] Therefore, there is a high probability that, in order to conduct an investigation, enforcement bodies may have to request some of these US entities for information. Although, we do not have a record of the number of requests that have been sent to these companies by enforcement agencies in India, we found that the UK government had sought customer data for at least 53,947 separate user accounts controlled by American technology companies in the year 2014.[285] Further, between January and June 2017, Google received 3,843 user data disclosure requests by Indian governmental agencies

[281] Shalini S., Evaluating MLATs in the Era of Online Criminal Conduct, CCG Working Paper Series No. 2 (2015-16).
[282] For some practical suggestions to make the MLAT regime effective, see Bedavyasa Mohanty and Madhulika Srikumar, Hitting Refresh: Making India-US Data Sharing Work, Observer Research Foundation Special Report No. 39 (2017) available at <https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf> (last accessed on 7 June 2018).
[283] According to Indiastat.com, India has an estimated population of 1,344,283,227 at present. The projected population for 2050 is 1,807,878,574, Estimated Population, Indiastat available at <https://www.indiastat.com/popclockflash.aspx > (last accessed on 8 April 2018).
[284] Alexa, Top Sites in India available at < https://www.alexa.com/topsites/countries/IN > (last accessed on 21 March 2018).
[285] Andrew Keane Woods, Against Data Exceptionalism, 68 Stanford Law Review (2016) at p. 743.

of which in 54% of the cases some data was produced.[286] Thus, Google refused to provide data in 46% of the cases.

It is not our claim that with a mandate to process data locally, perfect compliance will be achieved, and all requests will be automatically answered (or even, should be answered). This is because despite the data being located physically in India, a conflict of law question might arise if the country of the concerned entity's registration or any other country with which the entity or the claim is substantially connected, also asserts jurisdiction.[287]

However, if personal data that is within the remit of the data protection law is processed in India (in this case, personal data of persons present in India, collected by an entity outside India offering services to persons present in India or carrying on business in India), then the possibility of a foreign entity refusing access to such data would be reduced. Further, even if such access were denied, the fact of the physical location of the data being in India would be a key factor in a conflicts determination of which court will have jurisdiction over the matter. Thus, a requirement to store or process personal data locally would certainly aid domestic enforcement significantly and this can be achieved by requiring that at least one copy of the personal data be maintained within the territory of India.

(ii) Avoiding resultant vulnerabilities of relying on fibre optic cable network

A large amount of data is transmitted from one country to the other via undersea cables. For instance, Tata Communications owns and operates the world's largest subsea cable network which reaches a large number of countries representing 99.7 per cent of the world's GDP.[288] There have been studies which show that undersea cable networks are significantly vulnerable to attack.[289] A report by Policy Exchange highlights that sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to

[286] Google Transparency Report, Overview: India available at <https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:IN&lu=legal_process_breakdown&legal_process_breakdown= > (last accessed on 8 April 2018).

[287] In this context, the case of United States v. Microsoft, 584 US _ (2018) was argued in the US Supreme Court in February 2018. Law enforcement in the US claimed jurisdiction over personal data in relation to a crime in the US. The data itself was stored on a server in the Republic of Ireland. A jurisdictional question arose. For case history, see United States v. Microsoft Corporation, Oyez available at <https://www.oyez.org/cases/2017/17-2 > (last accessed on 9 May 2018). If there were a localisation mandate to store such data in the US, the case would have been rendered moot. As it happens, the question has become superfluous by the passage of the CLOUD Act by the US Congress.

[288] Tata Communications completes world's first wholly owned cable network ring around the world, Press Release - Tata Communications (22 March 2012) available at <https://www.tatacommunications.com/press-release/tata-communications-completes-worlds-first-wholly-owned-cable-network-ring-around-world/> (last accessed on 29 January 2018).

[289] Ryan Singel, Fibre optic cable cuts isolate millions from the Internet, Wired (31 January 2008) available at <https://www.wired.com/2008/01/fiber-optic-cab/> (last accessed on 29 January 2017); Alexandra Chang, Why undersea Internet cables are more vulnerable than you think, Wired (4 February 2013) available at <https://www.wired.com/2013/04/how-vulnerable-are-undersea-internet-cables/> (last accessed on 29 January 2017).

economic turmoil and civil disorder.[290] Further, the location of almost every undersea cable in the world is publicly available,[291] which increases the risk of vulnerability of the internet and cross-border transfer of data.[292]

From this, it may be argued that data critical to Indian national interest should be processed in India as this will minimise the vulnerability of relying solely on undersea cables. Critical data, in this context will include all kinds of data necessary for the wheels of the economy and the nation-state to keep turning. It is thus a wider category than the determination of data in respect of which foreign surveillance needs to be prevented and may include health, government services, infrastructure data and system control software which includes *inter alia* transport, waterways and all controlled and sensor mapped infrastructure. This may even extend beyond the scope of personal data, regarding which an appropriate call may have to be taken by the Government of India. The objective will be served if even a single live, serving copy of such critical personal data is stored in India. However, the processing of such data exclusively within India may be necessary for other benefits as discussed below.

(iii) Building an AI ecosystem

In the coming years AI is expected to become pervasive in all aspects of life that are currently affected by technology and is touted to be a major driver of economic growth.[293] For instance, a study by the consulting company Accenture has estimated that AI has the potential of adding 1.6 percentage points to China's economic growth by 2035 owing to China's recognition of the importance of AI and its commitment to investments in its development.[294] India's addition is expected to be USD 957 billion by 2035 (1.3 percentage points to be added to GDP).[295] Therefore, the economic potential of an AI ecosystem is immense.[296] Developments in this direction are thus integral to creating a thriving digital economy.

---

[290] Rishi Sunak, Undersea cables: Indispensable, Insecure, Policy Exchange (2017) available at <https://policyexchange.org.uk/publication/undersea-cables-indispensable-insecure/> (last accessed on 29 January 2017).

[291] Submarine Cable Map, Telegeography (2017) available at <https://www2.telegeography.com/submarine-cable-map> (last accessed on 29 January 2018).

[292] It may be noted that mandating the storage of all personal data locally could raise its own security concerns as the centralisation of all such data in one location would potentially make it more vulnerable, see for example, Anupam Chander and Uyên P. Lê , Data Nationalism, 64 Emory Law Journal (2015) at pp. 715-720. However, these concerns are of reduced significance because, as is discussed below, only a smaller sub-set of all personal data can be made subject to a mandate of local storage in India.

[293] Shripati Acharya, The great Indian data rush, Yourstory (26 February 2018) available at <https://yourstory.com/2018/02/great-indian-data-rush/> (last accessed on 23 April 2018).

[294] How Artificial Intelligence can drive China's Growth, Accenture (2018) available at <https://www.accenture.com/cn-en/insight-artificial-intelligence-china> (last accessed on 23 April 2018). For a more detailed analysis of the impact of AI on China's economic growth, see Artificial Intelligence: Implications for China, McKinsey Global Institute (April 2017) available at <https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx> (last accessed on 23 April 2018).

[295] Rewire for Growth: Accelerating India's Economic Growth with Artificial Intelligence, Accenture (2017) available at <https://www.accenture.com/t20171220T030619Z__w__/in-en/_acnmedia/PDF-68/Accenture-ReWire-For-Growth-POV-19-12-Final.pdf%20-%20zoom=50> (last accessed on 21 April 2018).

The growth of AI is heavily dependent on harnessing data, which underscores the relevance of policies that would ensure the processing of data within the country using local infrastructure built for that purpose. This is because currently most of the personal data of Indian citizens, such as the data collected by internet giants such as Facebook and Google are largely stored abroad.[297] Azmeh and Foster[298] in their 2016 study, point out the benefits that developing countries can derive from a policy of data localisation. These include: first, higher foreign direct investment in digital infrastructure and second, the positive impact of server localisation on creation of digital infrastructure and digital industry through enhanced connectivity and presence of skilled professionals. Creation of digital industry and digital infrastructure are essential for developments in AI and other emerging technologies, therefore highlighting the significance of a policy of requiring either data to be exclusively processed or stored in India. This benefit can be captured in a limited manner by ensuring that at least one copy of personal data is stored in India. Further, a requirement to process critical data only in India would create a greater benefit insofar as it extends beyond mere storage.

(iv) Preventing foreign surveillance

Finally, one of India's key interests with regard to personal data which is critical to India's national security interests and imperative for the smooth running of the wheels of the Indian economy is the prevention of foreign surveillance. It has been argued by some scholars that requirements of storing data within territorial borders may be useful in boosting data security by safeguarding the privacy and security of personal information against non-governmental actors.[299] Largely, major information intermediaries such as Facebook, Google, Amazon, Uber, etc. are headquartered in the US. Consequently, a significant portion of the data collected by some of these entities are stored in the US[300] and in other countries around the world thereby increasing the scope of foreign surveillance. Based on such access to the data or presence in a foreign jurisdiction, laws of foreign countries may potentially allow

---

[296] In fact, the Ministry of Commerce and Industry, Government of India has recognized the importance of AI and constituted a Task Force on Artificial Intelligence which has submitted a report on the subject, see Report of the Artificial Intelligence Taskforce available at <http://dipp.nic.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf> (last accessed on 7 June 2018).

[297] Shripati Acharya, The great Indian data rush, Yourstory (26 February 2018) available at <https://yourstory.com/2018/02/great-indian-data-rush/>(last accessed on 23 April 2018).

[298] Shamel Azmeh and Christopher Foster, The TIPP and the digital trade agenda: Digital industry policy and Silicon Valley's influence on new trade agreements, London School of Economics Working Paper No. 16-175, (2016) at pp. 26-27 available at <http://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf > (last accessed on 23 April 2018).

[299] See Jack Goldsmith, Unilateral Regulation of the Internet: A modest defence, 11(1) European Journal of International Law (2000); Alexander Savelyev, Russia's new personal data localization regulations: A step forward or a self-imposed sanction?, Computer Law and Security Review 32 (2016); John Selby, Data Localisation laws: trade barriers or legitimate responses to cybersecurity risks, or both?, 25(3) International Journal of Law and Information Technology (2017).

[300] Google Data Centres, Google available at <https://www.google.com/about/datacenters/inside/locations/index.html> (last accessed on 7 February 2018); Facebook Data Centres, available at <http://www.datacenterknowledge.com/data-center-faqs/facebook-data-center-faq > (last accessed on 7 February 2018).

surveillance. This is not fear-mongering — the PATRIOT Act amendments to FISA have precisely this effect.[301]

If data is exclusively processed in India, it will potentially cut off foreign surveillance of large amounts of such data. It is essential to recognise that the logical consequence of accepting this rationale is to advocate the processing of data only in India. Doing so for all kinds of data will create an Indian internet that will be walled away from the rest of the internet. Such a measure is clearly overbroad and hurts the prospect of a free and fair digital economy. Furthermore, it is not narrowly tailored to the type of data, surveillance of which is considered particularly detrimental. This would be precisely the kind of policy that ought to be avoided being based on ideological, as opposed to strategic, principled or practical considerations.

In order to strike a balance, it is essential to enquire into the kinds of surveillance activities that are most detrimental to national interest. In the context of personal data, this would pertain to such critical data as those relating to Aadhaar number, genetic data, biometric data, health data, etc. Only such data relating to critical state interests must be drawn up for exclusive processing in India and any such obligations should be limited to it. All other kinds of data should remain freely transferable (subject to the conditions for cross-border transfer mentioned above) in recognition of the fact that any potential fear of foreign surveillance is overridden by the need for access to information. Thus, for prevention of foreign surveillance critical personal data should be exclusively processed within the territory of India.

However, despite these advantages of partial or complete restrictions on cross-border flow of data, it is also important to consider the various costs that may be associated with the implementation of such a policy.

(b) Costs

(i) Economic and Market Implications

[301] Federal Bureau of Investigation, Testimony available at <https://archives.fbi.gov/archives/news/testimony/usa-patriot-act-amendments-to-foreign-intelligence-surveillance-act-authorities> (last accessed on 8 April 2018) "Section 207 of the USA PATRIOT Act changed the law as to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year…section 214 of the USA PATRIOT Act simplified the standard that the government must meet in order to obtain pen/trap data in national security cases… Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution"; see also, Sections 218 and 504 of the PATRIOT Act; Snowden disclosures helped reduce use of PATRIOT Act provision to acquire email records, The Guardian (29 September 2016) available at <https://www.theguardian.com/us-news/2016/sep/29/edward-snowden-disclosures-patriot-act-fisa-court> (last visited on 8 April 2018). Edward Snowden's disclosures have had the effect of curtailing the expansion of these provisions.

Any requirement to store and process data locally may impose a substantial economic burden on domestic enterprises that provide goods and services with the help of foreign infrastructure such as cloud computing.[302] One way of viewing this problem is to consider how the market would respond to such a mandate. Large foreign companies may be willing and able to invest in new servers within the territory where they want to operate. However, the costs of creating or renting such newly built infrastructure may be high for a number of small and medium-sized businesses (including domestic ones) that would otherwise have been able to afford cheaper foreign cloud service providers. By raising such entry barriers, such a mandate may thus aggravate existing issues like the monopolisation of the digital economy and monopolisation of data by foreign companies that have already been enjoying first-mover and network industry advantages in the last few decades. Allowing international flow of services would likely reduce the costs of data processing by small Indian companies looking to enter into the digital economy.

As discussed above, the representations made to us have not persuaded us of the possible economic implications of local storage and processing of personal data in India. It is our considered view that the size and potential of the Indian market trumps the additional cost that some entities may have to bear on account of a mandate to process personal data locally. Further, for small players, options of storing data on local clouds will only increase pursuant to our recommendation. Finally, by not making the requirement of processing of personal data in India absolute (applying to all kinds of data) and restricted to critical personal data (no transfer of data abroad), any onerous effects on smaller entities will be significantly obviated.

(ii) Balkanisation of the Internet and Domestic Surveillance and Censorship

Apart from the abovementioned considerations of data as a question of international trade and economic activity, the flow of personal data is specifically linked with the rights to free speech and privacy.

The availability of information about one nation in others has meant that the latter nations effectively become checks on the veracity and integrity of information in the former. Thus, if information about law enforcement actions against an individual in Country A is publicised from a website with servers in Country B, the government of Country A cannot compel or influence (including through the threat of force or sanctions) the website into modifying its information at the original copy in the servers.[303] On the contrary, mandating the processing of personal data locally might lead to harassment, censorship or worse still, self-censorship. Thus, some see this as a threat to free speech as all information about a country may become

[302] The weighted impact of localisation on the GDP of the EU is estimated to be about 0.4% (See An Economic Assessment of Data Localisation Measures in the EU Member States, European Centre for International Political Economy available at <http://ecipe.org/app/uploads/2016/12/Unleashing-Internal-Data-Flows- in-the-EU.pdf> (last accessed on 11 May 2018).

[303] See Jonah Hill, The Growth of Data Localisation Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders, The Hague Institute for Global Justice, Conference on the Future of Cyber Governance (2014) at p. 28 (finding that the internet has furthered, "individual participation in the political process, increased transparency of governmental activities, and promoted fundamental rights").

subject to filtering in a manner that was made impossible in the last couple of decades due to the rise of the internet.[304] The internet could get splintered into multiple subnets that are subject to more direct and comprehensive control by domestic governments with each being capable of covert control over content and accessibility. Domestic surveillance could also receive a substantial advantage as a result of increased access to the relevant data and the accompanying chilling effects can be greatly enhanced. In short, such a requirement of either requiring the maintenance of local copies of personal data or limiting the processing of personal data to India might derogate from the free and fair digital economy that we would like to create.

While this argument has a certain intuitive appeal, on reflection it suffers from certain logical flaws. First, merely because data is located in a country does not render it vulnerable to censorship. If censorship is indeed made possible, it requires, in addition, a dysfunctional data protection law that allows governments the tools to facilitate such censorship. It is certainly not an automatic consequence of local retention or restriction to local processing.

Second, several kinds of access restrictions take place today, without the requirement of local retention or processing, through blocking orders ('internet shutdowns'). The merits of such shutdowns are a distinct issue; the relevant point in this context is that access restrictions are possible without a mandate to store personal data locally as well.

Finally, the vision of several national internets entirely walled to the outside world is currently a caricatured characterisation that evokes fear of changing the status quo. So was the concept of the nation state bounded by territory and based on the principle of national sovereignty in the 17th century. If the unit in which sovereignty is vested and exercised is the nation state, it is inevitable that a movement towards making the nation state the central actor in internet governance will emerge.[305] The desirability of such movement cannot be assessed against the reference point of what the internet is today or was when it began. On the contrary, it requires a holistic assessment of the ongoing geopolitical changes in the world to understand what the internet might become. Thus, acting on a nostalgic understanding of what the internet was like when it started to defer a mandate to store and process personal data locally will be myopic. There is no principled or practical reason to believe that the very fact of local storage or restriction to local processing itself will make the digital economy any less free or fair. On the contrary, it will ensure more effective enforcement of substantive obligations that are directed towards these objectives. It will be free and fair, but possibly different from the internet we have today.

[304] Erica Fraser, Data Localisation and the Balkanisation of the Internet, 13(3) SCRIPTed available at <https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/> (last accessed on 14 May 2018); Christopher Kuner, Data Nationalism and Its Discontents, 64 Emory Law Journal (2014) at pp. 2089 and 2097; Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory Law Journal (2015) at pp. 677, 680 and 735.

[305] This is the basic argument made by Lawrence Lessig who talks of the future of internet regulation as "competition among sovereigns". Lawrence Lessig, Code: Version 2.0 (Basic Books, 2006) at pp. 306-310.

On the basis of the above discussion, it is the Committee's view that a three-pronged model should be followed. First, all personal data to which the law applies should have at least one live, serving copy stored in India. Second, in respect of certain categories of personal data that are critical to the nation's interests, there should be a mandate to store and process such personal data only in India such that no transfer abroad is permitted. Third, the Central Government should be vested with the power to exempt transfers on the basis of strategic or practical considerations thereby facilitating free flow of data across borders where justified. While these measures may not lead to perfect compliance, it is expected to significantly bolster domestic enforcement and reduce reliance on the MLAT request regime.

The Central Government should determine the categories of personal data for exclusive storage in India not just with regard to enforcement but also strategic interests of the State. Given the strictness of such an obligation, exceptions need to be laid down to allow for cross-border transfers even when exclusive storage is mandated. For instance, in respect of categories such as health data, cross-border transfers will have to be permitted where certain prompt action needs to be taken in order to protect the life or health of an individual. For example, the medical data of an Indian national may be transferred from one hospital in India to a hospital abroad where she is admitted for emergency treatment.

Transfers of critical personal data may also be permitted to those countries which have been green-lighted under the adequacy assessment for the purpose of cross-border transfers of personal data generally (as discussed above). However, the Central Government should only permit such transfers of critical personal data where necessary and provided that it does not hamper enforcement.

This model, in our view, strikes a harmonious balance between the interests of internet users, companies and the nation state in ensuring that data of persons present in India is both protected and used to empower them in their daily lives.

RECOMMENDATIONS

- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. **[Section 41(1)(a) of the Bill]**

- Intra-group schemes will be applicable for cross-border transfers within group entities. **[Section 41(1)(a) of the Bill]**

- The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA. **[Section 41(1)(b) of the Bill]**

- Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement. **[Section 40(2) of the Bill]**

- Personal data relating to health will however permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval. **[Section 41(3) of the Bill]**

- Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India. **[Section 40(1) of the Bill]**

CHAPTER 7: ALLIED LAWS

A. Impact on Allied Laws

The processing of personal data is omnipresent in the public and private sector. Currently norms relevant to data protection are spread across various statutes, which may lack overall consistency and general applicability. This creates ambiguity and irregularity in the protection of an individual's personal data. The proposed data protection framework must outline the minimum standards that will have to be followed and will have an impact on processing of personal data in all sectors, irrespective of more specific and overlapping sectoral statutes and regulations.

Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives. Data protection laws usually make room for the legislature to privilege particular objectives for the processing of personal data in specific situations. All such laws, however, will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. Similarly, the law will operate in tandem with extant legislation. In the event of any inconsistency, it will have overriding effect. In other words, no other law will operate in derogation of it. However, if a higher standard for protection of personal data is imposed by another law (for instance, the draft Digital Information Security in Health Care Bill, 2017), it may operate in addition to the proposed data protection law.

The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. **Annexure C** is attached to this report, listing such laws that may be affected. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.

Regardless of the overlapping effect of a data protection regime on other enactments, certain other enactments require to be amended simultaneously with a data protection regime. Three such enactments have been identified for disparate reasons. The Aadhaar Act needs to be amended significantly to bolster privacy protections and ensure autonomy of the UIDAI. Since the context of the Committee's functioning has been shaped by a vigorous public debate about Aadhaar and its impact on data protection, the Committee would be remiss if it did not deal with this issue. Second, the RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This has often been used to deny RTI requests in the past and requires harmonisation with the data protection framework proposed by us. Third, the data protection statute replaces Section 43A of the IT Act and the SPD Rules issued under this provision. Consequently, this provision requires to be repealed together with consequent minor amendments. Since the first two of these amendments require explanation, they are dealt with fully below.

B. Amendments to the Aadhaar Act

Much public attention around data protection issues has centred around Aadhaar and the possibility that creating a database of residents would be antithetical to a well-functioning data protection regime. The validity of arguments regarding its constitutional aspects has been litigated extensively in the Supreme Court in *Puttaswamy*.[306] Since the judgment is awaited, no comment is being made on the merits or demerits of such arguments and counter-claims.

However, it is salient that the data protection regime proposed by the Committee will require close introspection by the Government on various aspects pertaining to the existing functioning of the UIDAI. Currently the Aadhaar Act is silent on the powers of the UIDAI to take enforcement action against errant companies in the Aadhaar ecosystem. This includes companies wrongly insisting on Aadhaar numbers, those using Aadhaar numbers for unauthorised purposes and those leaking Aadhaar numbers, all of which have seen several instances in the recent past. Each of these can affect informational privacy and requires urgent redressal.

In addition, recent announcements of the UIDAI relating to the Virtual ID — creating an alias for authentication keeping the Aadhaar number out of the knowledge of the entity requesting authentication — and offline verification — allowing identity verification using QR codes without keeping a centralised record, have significant potential to ensure both collection limitation and data minimisation. However, there is no statutory backing for such announcements as on date and it is unclear as to how they are to be effectively implemented.

Amendments are thus necessary to the Aadhaar Act for bolstering privacy protections for residents as well as reconceptualising the UIDAI into a regulatory role that can ensure consumer protection and enforcement action against violations with appeals to an appropriate judicial forum. It is to be noted that this Committee is neither tasked with nor intends to suggest large-scale amendments to the Aadhaar Act itself. The amendments that are recommended are limited to those warranted by the need to bring the Aadhaar Act in line with the suggested data protection framework. These amendments, when read with several provisions in the draft data protection bill, particularly those in Chapter XI relating to penalties and remedies for aggrieved individuals, ought to alleviate data protection related concerns surrounding Aadhaar.

Accordingly, two broad sets of amendments to the Aadhaar Act are necessary:

First, amendments to bolster the right to privacy of individuals would be required. A critical obligation on all data fiduciaries is collection limitation, i.e. collection of personal data should be limited to such data necessary for processing. Accordingly, amendments have been suggested that classify requesting entities into two kinds to regulate access to personal data

[306] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India*, W.P. (Civil) No. 494/2012 Etc.

on the basis of necessity — those who can request for authentication and those who are limited to verifying the identity of individuals offline.

Regarding entities who can request for authentication, as a matter of principle, the same should be restricted to any entities which perform a public function and require verifiable identification for the purpose of performing such public function. This principle is captured by allowing any entity to request for authentication in two situations: first, if it is mandated by law made by Parliament. The Parliament, as the highest law-making body in the country is within its sovereign power to require individuals to authenticate themselves when it feels necessary. If any entity requests authentication pursuant to a parliamentary mandate, the same must be respected. It is expected that Parliament will be judicious in determining which entities require such authentication. Second, a public authority performing a public function that is approved by the UIDAI may also seek authentication. In granting such approval, the UIDAI should take into account security standards employed by the entity as well as the steps it has taken to incorporate privacy protections for Aadhaar number holders.

Further, the UIDAI may classify such requesting entities that are entitled to seek authentication into those which can directly access the Aadhaar number, i.e. authentication *simpliciter*, and those which can only access the Virtual ID, an alias of the Aadhaar number. The Virtual ID is a temporary 16-digit random number, which can be generated by an Aadhaar number holder for certain types of authentications. It does not reveal the individual's Aadhaar number. This distinction is significant to ensure that only those entities which require the Aadhaar number itself for their functioning, collect the Aadhaar number and other entities only collect the Virtual ID. This is how collection limitation can be upheld in the Aadhaar framework.

For entities which do not perform a public function, identification of individuals may still be necessary. Currently, many such entities, as a matter of course, ask for the Aadhaar number of individuals. This represents a significant privacy concern. For all such entities, only offline verification of Aadhaar numbers with the consent of the Aadhaar number holder may be used to verify the identity of an individual. This mechanism would ensure that sensitive information related to individuals such as their Aadhaar number is not disclosed to requesting entities for routine activities and transactions.

In this entire scheme, in order to ensure that privacy protection goes hand in hand with substantive benefits for individuals, all requesting entities are mandated to ensure that in case there is an authentication failure owing to *bona fide* reasons such as infirmity, disability or technical failure, alternate means of identification (such as offline verification or others) should be made available. This has been made obligatory on all requesting entities. Further, it has been reiterated that core biometric information shall not be shared with anyone as the highest standard of protection is necessary for it.

Second, amendments are required to ensure the autonomy of the UIDAI. With over 121 crore Aadhaar numbers having been issued, the Government of India and State Governments

making Aadhaar authentication mandatory for several benefits, subsidies and services, and several private transactions using Aadhaar as a method of identification, the need of the hour is a regulatory framework for the operation of Aadhaar. This requires two conceptual changes to the way in which the Act currently conceives of the UIDAI— first, the UIDAI must be autonomous in its decision-making, functioning independently of the user agencies in the government and outside it, that make use of Aadhaar; second, the UIDAI must be equipped with powers akin to a traditional regulator for enforcement actions.

After having examined the powers and functions of existing statutory regulators such as TRAI, SEBI, CCI, etc. and the deficiencies in the existing framework for Aadhaar, the Committee is of the considered view that the UIDAI must be vested with the functions of ensuring effective enforcement, better compliance, consumer protection and prevention and redress of privacy breaches. Accordingly, powers should be given to the Authority to impose civil penalties on various entities (including requesting entities, registrars, and authentication agencies) that are errant or non-compliant. In cases involving statutory violations or non-compliance, or an actual or impending privacy breach, the UIDAI will be tasked with the power to issue directions, as well as cease and desist orders to state and private contractors, and other entities discharging functions under the Aadhaar Act.

This will work in tandem with the provisions of the draft data protection bill which will allow all aggrieved individuals to approach the Data Protection Authority in case of violation of the data protection principles, against any entity in the Aadhaar ecosystem, including the UIDAI itself, when it is a data fiduciary. Taken together, this will ensure that aggrieved citizens have appropriate remedies against all entities handling their Aadhaar data and errant entities in the Aadhaar ecosystem are subject to stringent enforcement action.

Finally, to bolster the financial autonomy of the UIDAI as a regulator, amounts received from penalties levied by the Authority under the Act will be deposited in a separate fund. This is critical if UIDAI is to play the role of a responsible regulator and a responsible data fiduciary.

The proposed changes will be instrumental in addressing significant privacy concerns that have been raised relating to the Aadhaar framework. They will also ensure that the UIDAI is more autonomous in its functioning, and has the necessary regulatory tools to protect privacy interests of Aadhaar number holders. Finally, in its role as a data fiduciary under the proposed data protection framework, the UIDAI will, in the eyes of the data protection law, be viewed as any other entity processing personal data of individuals, and will be subject to the rigours and penalties of the law. It is thus critical that these changes be made hand-in-hand with a new data protection legislation.

To make the aforementioned changes, it would be necessary to carry out certain amendments to the Aadhaar Act on the lines of the suggestions made in the Appendix to this Report. The Government may consider such amendments as it may deem appropriate and take suitable legislative measures to implement them.

C. Amendments to the RTI Act

Data protection law is designed to limit the processing of personal data to legitimate reasons where the flow of information is beneficial and respects the autonomy of the data principal. It is particularly sensitive to the harm to an individual pursuant to the disclosure of personal data and seeks to actively prevent such harm.

However, disclosure of information from public authorities may lead to private harms being caused. It is thus important to recognise that, in this context, there is a conflict of fundamental rights, between transparency and privacy. This requires careful balancing. The fact that neither the right to privacy not the right to information is absolute and will have to be balanced against each other in some circumstances has been recognised by the Supreme Court.[307] This balance is sought to be achieved by the exemptions in Chapter II of the RTI Act.

Chapter II of the RTI Act grants citizens a right to obtain information from public authorities and a procedure is put into place for dealing with requests for such information. However, certain exemptions are provided for in Section 8 of the Act in which case the disclosure of the requested information is not necessary.

Of relevance is the exemption in Section 8(1)(j) which reads:

> (1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen, --
>
> (j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information.
>
> *Provided* that the information which cannot be denied to the Parliament or State Legislature shall not be denied to any person.

The section creates a test which balances the right to privacy of a person against the right of a third party to seek information. The section requires the Public Information Officer to generally provide information, unless such information has no relationship to any public activity or interest or causes unwarranted invasion of privacy. These tests may sometimes work against the interests of transparency. To give an illustration, the Supreme Court has

[307] *Thalapallam Ser. Coop. Bank Ltd.* v. *State of Kerala* (2013) 16 SCC 82 ("Right to information and Right to privacy are, therefore, not absolute rights, both the rights, one of which falls under Article 19(1)(a) and the other under Article 21 of the Constitution of India, can obviously be regulated, restricted and curtailed in the larger public interest. … Citizens' right to get information is statutorily recognized by the RTI Act, but at the same time limitations are also provided in the Act itself …")

held that the *performance of an employee/officer in an organisation is primarily a matter between the employee and the employer and normally those aspects are governed by the service rules which fall under the expression "personal information", the disclosure of which has no relationship to any public activity or public interest.*[308] While releasing documents such as Annual Confidential Reports may not be desirable in all circumstances,[309] it is questionable whether the performance of a public servant is indeed a matter which has no relationship to any public activity or interest. If the condition that the information bears no relation to any public activity or public interest is met, the burden shifts on the seeker of information to establish that the disclosure of the information is in larger public interest.[310] This may often be a difficult burden to bear as the citizen may not be in possession of any material to establish any specific concern involving larger public interest. Further, this defeats the spirit of the RTI Act which sees transparency as an end in itself, and not necessarily a means to an end.

The other condition in Section 8 (1)(j) for denial of information, i.e. "which would cause unwarranted invasion of privacy" also raises complex issues. First, there is no indication in the provision as to what constitutes an unwarranted invasion of privacy. This problem may be exacerbated by the enactment of a data protection law which gives a broad definition of personal data. A lot of information sought from a public authority may contain personal data of some kind or another. Further a strict interpretation of purpose limitation may give rise to the inference that any disclosure other than for the purpose for which the personal data was submitted would lead to an unwarranted invasion of privacy. For instance, if a citizen entertains a well-founded suspicion that an unqualified candidate has been appointed to a post by a public authority, she would be well within her right to seek information relating to educational qualifications submitted by the employee as part of the recruitment process. That such personal data was submitted for the purposes of evaluation *alone* should not be a bar to disclosure for being contrary to the purpose limitation provision of the data protection bill.

To avoid this predicament, the RTI Act must specifically spell out the circumstances in which disclosure of such personal information would be a proportionate restriction on privacy having regard to the object of the RTI Act in promoting transparency and accountability in public administration.[311] This must be done keeping in mind the fact that the RTI Act generally leans in favour of disclosure of information.[312]

The fact that information is in the custody of a public authority gives rise to a presumption that it is information available to a citizen to access. The burden then falls upon the public authority to justify denial of information under one of the exceptions. This is a critical feature of the design of the RTI Act and the Committee finds that this must be preserved notwithstanding a data protection law.

---

[308] *Girish Ramachandra Deshpande* v. *Central Information Commissioner* (2013) 1 SCC 212.
[309] *RK Jain* v. *Union of India* (2013) 14 SCC 794.
[310] *Girish Ramachandra Deshpande* v. *Central Information Commissioner* (2013) 1 SCC 212 para 13.
[311] See long title of the Right to information Act, 2005.
[312] *Surupsingh Naik v. State of Maharashtra* (2007) 4 Mah LJ 573.

The question then arises as to what are the exceptional circumstances in which personal data can be denied to a citizen. Here, the relevant factor should be any likely harm that may be caused to the data principal by the disclosure of such information. As noted above, the RTI Act, in most circumstances, leans in favour of disclosure, underlining the importance of transparency in public activities. The Committee is cognizant of the fact that this feature of RTI Act has contributed tremendously to securing the freedom of information and enhancing accountability in public administration. This feature has to be accounted for in any balancing test created under the RTI Act. Therefore, in addition to the likelihood of harm, disclosure should be restricted only where any likely harm outweighs the common good of transparency and accountability in the functioning of public authorities.

Accordingly, the proposed amendment to Section 8(1)(j) has three features:

First, nothing contained in the data protection bill will apply to the disclosure under this section. This is to prevent privacy from becoming a stonewalling tactic to hinder transparency.

Second, the default provision is that the information which is sought must be disclosed. It is assumed that such disclosure promotes public interest and the common good of transparency and accountability.

Third, only if such information is likely to cause harm to a data principal and such harm outweighs the aforementioned public interest, can the information be exempted from disclosure.

The Committee finds that such a formulation offers a more precise balancing test in reconciling the two rights and upholding the spirit of the RTI Act without compromising the intent of the data protection bill.

RECOMMENDATIONS

- Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives.

- All relevant laws will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. In the event of any inconsistency between data protection law and extant legislation, the former will have overriding effect.

- The proposed data protection framework replaces Section 43A of the IT Act and the SPD Rules issued under that provision. Consequently, these must be repealed together with consequent minor amendments. **[First Schedule of the Bill]**

- The RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This needs to be amended to clarify when it will be activated and to harmonise the standard of privacy employed with the general data protection statute. **[Second Schedule of the Bill]**

- The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.

- The Aadhaar Act needs to be amended to bolster data protection. Suggested amendments for due consideration are contained in the Appendix to this Report.

CHAPTER 8: NON-CONSENSUAL PROCESSING

Despite the importance of consent in the legal framework, reasons other than consent may, on occasion, be relevant bases for processing of data. This is consistent with our normative framework— while consent, as an expression of autonomy is constitutive of a free and fair digital economy, so are other interests. Thus, it is only a combination of individual autonomy together with such other valuable interests that make a free and fair digital economy possible and it is only in such a normative framework that autonomy and such other interests are meaningfully protected.[313]

The critical question for determination in the law would be what the circumstances are where consent is either not appropriate, necessary, or relevant for processing. To understand the nature of the interests owing to which non-consensual processing will be permitted, a useful starting point would be the *Puttaswamy* judgment. Chandrachud, J., identified four 'legitimate state interests' to be considered in the context of privacy. He listed 'national security', 'prevention and investigation of crime', 'protection of revenue' and 'allocation of resources for human development' of which the first three are straightforward state functions that serve collective interests. The fourth which pertains to allocation of resources for human development with the aim of preventing wastage of public resources belongs to a distinct category and is considered under the head 'functions of the State'.

In addition to the illustrative list of "legitimate state interests" provided by Chandrachud, J., two other interests may be equally weighty—ensuring compliance with law and complying with a judicial order. Further, non-consensual processing may be relevant to the promotion of a free and fair digital economy in matters relating to use of personal data for journalism and purely domestic or personal purposes. While these are not state interests, they are societal interests which are better served by the free flow of information without hindrance. Finally, certain weighty individual interests may also override the consent requirements of this law, such as prompt action to save the life of an individual need not adhere to the terms of consent as per this law. Needless to say, other obligations on data fiduciaries may continue to apply.

It is necessary to note that this chapter deals with two categories of processing that are ordinarily dealt with separately in law: (i) grounds other than consent for processing; and (ii) exemptions from the law.[314] This conflation is deliberate for the purpose of conceptual clarity — each of these cases, whether processing for national security or prompt action to save the life of an individual, is characterised by the fact that a non-consent based ground for processing is used. However, an important distinction must be drawn between the non-consensual grounds of processing and exemptions. Grounds of processing represent non-consensual bases for processing of personal data that address situations where it is not

[313] This is not a utilitarian argument that is sacrificing individual interest for collective interest. Rather it is a Razian argument that all such interests together constitute a notion of the common good. See Joseph Chan, Raz on Liberal Rights and the Common Good, 15(1) Oxford Journal of Legal Studies (1995).

[314] Such a framework has been followed by the EU GDPR which specifically provides non-consensual grounds of processing and thereafter lays downs specific categories of exemptions in the law.

possible to obtain consent or consent may not be an appropriate ground for processing. All other obligations under the law are ordinarily applicable to such processing and any incursion into privacy is minimal. Most exemptions, on the other hand are non-consensual grounds of processing which are exempt from substantive obligations under the law and constitute restrictions on the right to privacy.

Non-Consensual Grounds for Processing

A. White Paper and Public Comments

The White Paper suggested that grounds for processing other than consent should be recognised since it is not always possible to obtain consent in all situations.[315] Grounds such as performance of contract and necessity for compliance with law were considered to be intuitively necessary.[316] A suitable adaptation of the "legitimate interest" ground in the EU GDPR was suggested for India.[317] The White Paper was of the view that there should be a residuary ground under which data could be processed, as it was not possible for a data protection law to foresee all situations which may warrant the processing of personal data without seeking consent.[318] Commenters overwhelmingly agreed with the need for recognising grounds for processing other than consent. Several commenters were however of the opinion that the law should be prescriptive, and no residuary ground should be retained due to possibility of interpretational ambiguities. One of the alternatives suggested to a "grounds of processing approach" was a two-tiered model based on: (i) legitimate purpose where data could be processed without consent (based on grounds such as legal necessity, to undertake certain risk mitigation activities, to carry out judicial and administrative orders, to carry out processing activities necessary for the prevention and detection of illegal activities and fraud); and (ii) a rights-based framework where once consent had been given, the data fiduciary would ensure that data was being processed in a manner which would not violate the rights of the individual, including the right to be treated fairly and without bias, the right of the individual to seek information relating to the uses to which her personal data would be put or disclosed, and that such data would be processed in accordance with the highest standards of security and safety.[319]

B. Analysis

[315] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 103.
[316] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 103.
[317] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 104.
[318] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 104.
[319] Comments in response to the White Paper submitted by Shivakumar Shankar, Managing Director of LexisNexis Risk Solution, 30 January 2018, available on file with the Committee.

Based on a review of academic literature, international best practices and comments received in response to the White Paper, the Committee has identified the following non-consensual grounds for processing which are relevant to the Indian context. The scope and description of these grounds of processing are set out below.

I. Functions of the State

(a) Context

As has been pointed out before, a data protection law, to be meaningful should, in principle, apply to the State. It would indeed be odd if a law enacted to give effect to a fundamental right to privacy does not serve to protect persons from privacy harms caused by processing of personal data by the State.

While for several interactions with the state, consent would be the norm for processing of personal data, the suitability of consent as a ground for processing of personal data by the state performing a state function, raises several questions. Some functions of the state are of a nature that consent may not be an appropriate ground for processing. In several situations, where the State interacts with the citizen, the imbalance of power between them would very often affect the validity of the consent given. The ongoing debate about Aadhaar squarely raises this issue. When a citizen is to receive a welfare benefit, the validity of any consent given is questionable. The problem is exacerbated if the consent is given by a person in dire need of essential services or goods. The interaction between the state and the citizen in this context cannot be compared to that of a consumer entering into a contract with a service provider. The option available to a consumer in refusing an onerous contract and choosing another service provider is not available to a person seeking a welfare benefit from the state.

Similarly, the State also collects large amounts of personal data in the performance of its regulatory functions. For instance, the approval of a building permission by a local body is subject to the submission of an application which is bound to contain personal data of the applicant. Any attempt to obtain consent, particularly where a citizen or person seeks approval from the State is bound to be reduced to a formality. If on the other hand, genuine consent is to be operationalised in these circumstances, collective interests stand to suffer. For instance, from the last example, few would argue that a building permission can be given even if information necessary to evaluate the plan is withheld by the applicant.

There may be other situations where the state may need access to various data sets for performing certain functions. For example, one of the functions of a District Planning Committee, as per various State District Committee Planning Acts, is to prepare a suitable employment plan.[320] In furtherance of this goal, the District Planning Committee may collect

[320] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, (2017) at p.7; UK Information Commissioner's Office, When is consent appropriate? available at https://ico.org.uk/for-

personal data of individuals in the district as part of this exercise. If such a function is to be conditional on consent, and such consent is to meet the standard discussed above, it would be open to persons to not participate in the exercise, thus skewing the accuracy of the data set.

Mindful of the functions of the State, various jurisdictions have created non-consensual grounds of processing personal data in exercise of public functions. For example, in the EU the ground of processing of public function of the State applies when a public authority carries out its tasks, duties, functions and powers (including its discretionary powers). These functions are required to be those that have been set out under law.[321] Such law need not necessarily be an explicit statutory provision.[322] The ground would be relevant so far as the law's application is clear and foreseeable for the overall purpose for which the public function is to be carried out and a legal basis for each specific activity within such purpose may not be needed.

As per the EU GDPR, the relevant task or function that the public authority is performing should nonetheless have a basis in law. The lawful basis of such a public function should be documented and the official authority acting as data fiduciary should be able to identify a basis, for example in statute or common law for the activity for which they process personal data.[323] Therefore, a public function of the state can be carried out only if it is in furtherance of such law. Consequently, any processing that is undertaken by the official authority beyond what is envisaged under law would not be permitted under this ground of processing. It is imperative to draw a distinction between 'public function' and 'compliance with law'. While the latter restricts processing to mandatorily comply with the letter of the law, "public function" extends it to performing acts which are in furtherance of the law through a grant of powers or discretion.

If the public authority in question is able to demonstrate that it is exercising its lawful and legitimate authority and that the processing is necessary for such exercise, there is no additional obligation on such authority to prove that the purpose is actually part of a public function. In this instance, the term "necessary" would mean that the processing should be targeted and proportionate to the purpose.

A natural extrapolation of the above principle is that an organisation which is deemed to be a public authority could rely on this ground to carry out processing of personal data but is necessarily limited by its lawful functions. Where activities are excluded from the scope of an authority's legally prescribed public function, the authority would have to rely on consent or some other ground of processing.

---

organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/ (last accessed on 13 July 2018).

[321] Article 6(3), EU GDPR.

[322] Recital 41, EU GDPR.

[323] UK Information Commissioner's Office, Public Task available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/> (last accessed on 7 May 2018).

(b) Scope

In determining the scope of non-consensual processing by the state in India, regard must be had to three factors: the nature of the entity performing the function, the nature of the function and last, the extent to which personal data can be processed. All three factors must be satisfied in accordance with the discussion below for non-consensual processing to apply.

First, only bodies covered under Article 12 of the Constitution may rely on this ground. The established jurisprudence of Article 12, including the meaning of 'other authorities' under the Article would create an adequate check on the kinds of bodies that may process personal data.[324] Illustratively, these entities include ministries and departments of the Central and State Governments, bodies created by or under the Constitution, Parliament, and State Legislatures. These entities are assigned specific functions of governance but may also carry out activities that are private in nature. The latter should not be the basis for processing under the ground. Processing towards such activities, including by government companies, will not be permitted under this ground as the second factor to be satisfied, i.e. that it is for the performance of a public function, will not be met.

Second, permitting non-consensual processing by entities above for all kinds of public functions may be too wide an exception to consent (private functions being performed by these bodies are anyway excluded from this ambit). The Supreme Court, in *Puttaswamy*, while commenting on the need for non-consensual processing of personal data by the State observed:

> *In a social welfare state, the government embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But, the data which the state has collected has to be utilised for legitimate purposes of the state and ought not to be utilised unauthorizedly for extraneous purposes. This will ensure that the legitimate concerns of the state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology – legitimately deployed is a powerful enabler in the spread of innovation and knowledge*.[325]

[324] Ajay Hasia v. Khalid Mujib (1981) 1 SCC 722; Pradeep Kumar Biswas v. Indian Institute of Chemical Biology (2002) 5 SCC 111; Zee Telefilms v. Union of India (2005) 4 SCC 649.
[325] Puttaswamy, (2017) 10 SCALE 1 at para 181.

Drawing from the above observation, it is possible to envisage processing of personal data for two particular kinds of functions. First, personal data may be collected to the extent necessary for the provision of any service or subsidies in the nature of welfare benefits. Second, the State should be allowed to collect personal data to the extent necessary for the performance of regulatory functions. Such functions are, undoubtedly, intrinsically linked to ensuring governance. These could include the issuance of licenses, permits or approvals by the Executive. An extensive exercise may need to be carried out for the identification of the various bodies within the Central Government and State Governments that constitute data fiduciaries as well as to demarcate specific functions of such bodies for which this ground can be relied upon. Here, it important to stress that only those bodies which are performing functions directly connected to such activities should be allowed to use this ground. Further, such functions must be specifically authorised by law. A large part of the functioning of various departments of Government may be indirectly or remotely connected to the promotion of public welfare or regulatory functions. The ground cannot be used to justify the processing of personal data for all such functions. For functions not covered under this ground, the State, like other private actors, must rely on consent as the ground for processing personal data.

Third, while processing personal data under this ground, the state should not collect personal data more than what is necessary for a legitimate purpose. In the case of consent, a data fiduciary can potentially collect personal data even beyond what is strictly necessary for any task, where the data principal consents to such collection. Processing of data by the state on the basis of a non-consensual ground must be strictly confined by necessity. The State should not collect more personal data than what is necessary for any stated purpose and any systematic collection of data is to be preceded by an assessment of the extent to which data collection would be proportionate having regard to the legitimate purpose at hand. This requires to be stressed in the context of the provision of welfare benefits. Processing of personal data should, in no case, take the form of a coercive measure to collect more information than is necessary for any legitimate purpose associated with the provision of such benefit. Any such processing would fail to meet the requirement of fair and reasonable processing under the law.

(c) Application of Obligations

As is clear from the observation in *Puttaswamy*, it is the strict application of data protection obligations which will ensure that the personal data of citizens and other data principals are not misused even where such processing is non-consensual. Thus, even in those situations where the State may insist on the collection of data for certain functions, the state should rigorously abide by data protection obligations. Particular regard should be had to principles such as data minimisation, purpose limitation and transparency. The state should provide clear notice of purpose when it collects data from citizens and processing must be confined to the stated purposes and must be carried out in a transparent manner. Given the higher standards of accountability expected of the state,[326] it is only such fair and reasonable processing that will enable citizens and other data principals to trust the state with their personal data.

II. Compliance with Law or Order of Court or Tribunal

(a) Context

There are certain legal obligations which involve the processing of personal data, either for the fulfilment of a purpose or direction outlined in law or compliance with an order of a court or tribunal. Similarly, personal data that is processed pursuant to a court or tribunal order would be covered. Such collection will be justified under the ground of compliance with a law or order of court or tribunal. It is important to have this ground of processing in order to ensure that the data protection law does not hinder the application of obligations and compliances under other laws and the adjudicatory system. Realising the importance of the same, a number of countries have recognised this ground of processing.[327]

This ground will not apply if the collection, use or disclosure of personal data is not mandatory under a valid law or order of a court or tribunal. For example, if personal data is

[326] Even in matters of contract, the State is expected to be fair and cannot act like a private body. *New Horizons Limited* v. *Union of India*, 1995 (1) SCC 478

[327] Article 6(3), EU GDPR; Recital 41, EU GDPR; Information Commissioner's Office, Legal Obligation available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/> (last accessed on 5 May 2018); Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19; Sections 11 and 12 POPI Act; Section 1, South African Revenue Service Act, 1997; Section 84 read with Schedule 9 (3) of the UK Data Protection Bill. The EU GDPR permits processing when it is necessary for the compliance with a legal obligation. The legal obligation need not necessarily be an explicit statutory obligation. Therefore, delegated legislation in the form of rules and regulations and common law obligations will also constitute law as long as the application of the law is foreseeable to those data principals subject to it. However, processing of data beyond what is required by law through voluntary unilateral engagements and public-private partnerships will not be permitted. In South Africa, personal information may be processed if processing complies with an obligation imposed by law on the responsible party. Further, personal information need not be collected from the data subject if it is required to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue. The UK Data Protection Bill contains a provision similar to the EU GDPR wherein processing is allowed as long as it is necessary for compliance with a legal obligation to which the controller is subject, other than an obligation imposed by contract.

used or disclosed under a contract, this ground would not be applicable.[328] Further, this ground of processing will only extend to laws passed by Parliament or State Legislatures and subordinate legislation therein, and orders of courts or tribunals in India. It will not cover a duty or obligation of data fiduciaries arising out of a foreign law, treaty or international agreement (unless such duty or obligation is also specifically recognised through domestic law), or orders delivered by foreign courts.

(b) Scope

In our view, a separate ground for compliance with law or order of court or tribunal should be recognised in order to avoid inconsistency with obligations under other laws and judicial orders. The word 'law' shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications as per Article 13 of the Constitution (with the exception of custom and usage). However, processing under any rules, notification or any other delegated legislation must be based on some statutory authority. Obligations imposed by contract and foreign law shall not be permitted to be processed under this ground. An order of court or tribunal would be restricted to Indian courts and tribunals. Processing of sensitive personal data may be permitted only if it has been explicitly mandated under any law made by Parliament or the Legislature of any State or order of a court or tribunal in India.

The Committee notes that there may be some overlap between the ground permitting non-consensual processing in compliance with law and the ground relating to functions of the state discussed above. This ground accommodates processing of personal data which has been made mandatory under any law. This may be undertaken by private actors acting in compliance with a law. For instance, a company is required to file annual returns which may contain personal data of individuals such as promoters, directors or key managerial personnel.[329] It would be superfluous for a taxation authority to seek consent of an assessee before collecting information when such collection has been made mandatory under a law. As with the previous ground, what is critical is the amount of information which can be collected under any such law. Any statute mandating processing of personal data must meet the requirement of proportionality to be constitutional vis-à-vis the right to privacy.

(c) Application of Obligations

It should be noted that if processing is undertaken under this ground, it must comply with the data protection law in general.[330] Obligations such as purpose limitation and collection limitation will apply since personal data may only be collected as sanctioned by the law or judicial order under which the data is being collected and processed. In other words, the data

[328] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19.

[329] Section 92 of the Companies Act 2013.

[330] More specifically, the requirements of necessity, proportionality and purpose limitation; See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 19.

protection law will supplement all existing laws permitting data collection so as to ensure that any processing of personal data respects the right to informational privacy of citizens. The only exception to this principle will be where a statute has explicitly prescribed higher norms of data protection in which case, such obligations can apply to the exclusion of provisions under this law.

As with the previous ground, the right to data portability may not be suitable since the entity maintaining the personal data is likely to be doing so for a purpose which may not allow for the transfer or deletion of such data. Thus the right to data portability will not apply in these two non-consensual grounds for processing.

III. Prompt Action

(a) Context

There may be cases where an individual's personal data may be processed in an emergency health situation, or when there is a significant risk to the individual's health and safety. In such cases, seeking consent prior to processing may be onerous, or entirely impossible. For instance, rescue operations, transporting a road accident victim to the hospital, contacting the next of kin of a dying person, and large-scale rescue operations during natural disasters would fall under this category. To permit processing in such situations, it is necessary to have a ground for prompt action.

It is important to note that while the application of this ground is limited to particular situations involving questions of life and death of the data principal and threat of injury, it is not necessary for such threat to be immediate.[331] Therefore, this ground of processing can be used for collecting, using or sharing data in situations when the harm is not immediate such as when there is a threat of epidemiological disease.[332] Moreover, this ground can be used in situations when there is risk of significant harm to life,[333] where processing is necessary for humanitarian emergencies (disaster management) and where processing is necessary to protect the data principal's life or health. The importance of this ground is further bolstered by the fact that a number of countries have recognised it.[334]

---

[331] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 20.

[332] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014) at p. 20.

[333] Data Protection and Sharing- Guidance for Emergency Planners and Responders available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf (last accessed on 6 May 2018).

[334] Article 6(d), EU GDPR; Article 9 (2) (c) read with Recital 112, EU GDPR; Section 76 read with Schedule 10 (3), UK Data Protection Bill; Section 11(d), POPI Act. As per the EU GDPR, this ground is permitted to be used where processing is necessary in order to protect the vital interests of the data principal or of any other person. Additionally, in situations where 'processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent', the ground of vital interest may be invoked. The UK Data Protection Bill has a provision similar to the EU GDPR. In South Africa, processing is permitted if it protects the legitimate interest of the data principal. Therefore, while the

(b) Scope

The Committee is of the view that this ground should be extended to the following situations: (i) where there is a threat to life or health of a data principal; (ii) for provision of medical treatment or health services to individuals during an epidemic, outbreak of disease or any other threat to public health; and (iii) for ensuring safety of individuals and to provide assistance or services to individuals during any disaster or during a breakdown of public order. It should only be invoked when it is impractical or impossible to use any other ground for processing. Further, it should be strictly interpreted and must only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary for fulfilling any of the aforementioned situations. Processing of certain categories of sensitive personal data such as sex life, sexual orientation, caste or tribe, or religious or political affiliation or belief, transgender and intersex status however should not be permitted under this ground as they would not be relevant to any measures of prompt action.

(c) Application of Obligations

Notice provisions, as laid out in the data protection law shall not be applicable to processing carried out under this ground, if it substantially prejudices the purpose for such processing. All obligations relating to purpose limitation, collection limitation, storage, accuracy, security safeguards and the data principal rights shall continue to apply since personal data processed in an emergent situation should be limited to the purposes it was processed for and must be securely kept for as long as is necessary and disposed of thereafter.

IV. Employment

(a) Context

There are a large number of situations where an employer may find it necessary to process personal data pertaining to their employees or to their potential employees. For instance, employers may need to collect personal data from individuals for the purpose of recruitment. This may include personal data such as the names, addresses and educational qualifications that a potential candidate might include in her application form. Employers may also find it necessary to process personal data of their employees during the course of their employment relationship, which might include bank account details, PAN card numbers etc. for the purpose of paying their salaries. Other personal data, which an employer may collect and process may include medical records, records pertaining to promotions, disciplinary matters, attendance records and so on. In many situations, processing activities in relation to the above could be carried out on the basis of consent of the individual or even on the ground of

scope of application is wider than the EU model, it is limited to only the data principal whereas the EU GDPR extends vital interest to "any other person" as well.

legal compliance, where the employer is required or authorised by law to collect, disclose[335] or process certain types of personal data.

However, these grounds alone may not be sufficient or appropriate in certain circumstances for the purpose of carrying out processing activities in the context of employment. For instance, the data protection law sets out that for consent to be valid, it must be free, informed, clear, specific and capable of being withdrawn. By this logic, employees are seldom in a position to freely give, refuse or revoke consent due to the nature of the relationship between the employer and the employee and the inherent dependency of the employee on the employer.[336] There may also be several processing activities which require the employer to seek consent from the employee multiple times, or on a regular basis. Seeking consent in this manner may involve a disproportionate effort on the part of the employer or may lead to consent fatigue on the part of the employee.

Further, relying solely on compliance with law as a ground for processing in an employment context is also not adequate as there are many other types of personal data such as collection of attendance records which are not mandated by law.

(b) Scope

The Committee is of the view that this ground should be extended to the following situations: (i) recruitment or termination of employment of a data principal; (ii) provision of any service to or benefit sought by an employee; (iii) verifying the attendance of an employee; or (iv) any other activity relating to the assessment of the performance of the employee. This ground should be invoked only where it involves a disproportionate or unreasonable effort on the part of the employer to obtain valid consent of the data principal, or where validity of the consent is in question due to the unique nature of the relationship between the employer and employee. This ground may be used when the type of processing activity which is required to be undertaken by the employer does not fall within any of the other grounds.

(c) Application of Obligations

All obligations will be applicable on data fiduciaries who are carrying out processing activities in the context of employment. Therefore, the employer must adhere to the principles of collection limitation and purpose limitation and collect only as much personal data as may be required to satisfy their purpose. The employer, as a data fiduciary, must also

[335] Section 45(2)(c), Employees' State Insurance Act, 1948 stipulates that an employer may be required to furnish books, accounts and other documents relating to the employment of persons and payment of wages upon request to the Social Security Officer. Similarly, Section 13(2)(a), Employees' Provident Funds and Miscellaneous Provisions Act, 1952 provides that an Inspector has the power to require an employer to furnish such information as may be necessary.

[336] Article 29 Data Protection Working Party, Opinion 02/2017 on data processing at work at p. 3; Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, (2017) at p.8; UK Information Commissioner's Office, When is consent appropriate? available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/ (last accessed on 13 July 2018).

adopt any such organisational measures as may be necessary in order to safeguard the personal data being processed. Other obligations such as storage limitation and accuracy will also apply to the employer.

The employer should give employees sufficient notice detailing the personal data being collected, the purpose for which it is being processed, and the third parties to whom such data may be disclosed and so on. Further, data principal rights of confirmation, access, correction and portability will also be available to the employees.

V. Reasonable Purpose

(a) Context

There is a need for a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The primary advantage of having "reasonable purpose" as a ground of processing is the flexibility it affords to data fiduciaries.[337] This ground would be applicable in situations where data fiduciaries may need to carry out processing for prevention and detection of unlawful activities including fraud, whistleblowing, and network and information security, where it may not be possible to take consent in all situations. Resorting to consent in such situations, as a ground for processing may prove burdensome and may raise concerns of consent fatigue among data principals. Furthermore, relying on consent may hinder the evolution of new technologies relying on data analytics, which may hold significant benefits.[338]

(b) Scope

Various processing activities may fall under the ground for reasonable purpose, ranging from processing for the benefit of the data principal to processing for the mutual benefit of the data principal and the data fiduciary.[339] The need for this ground can be broadly understood through the following illustrations:[340]

(i) Fraud prevention: An insurance company wishes to process personal data for anti-fraud measures. Seeking consent of the concerned individuals could

[337] See UK Information Commissioner's Office, Legitimate Interests available at < https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/> (last accessed on 3 April, 2018). Legitimate interests (as the EU GDPR refers to this ground of processing) is the most flexible lawful basis for processing.

[338] Federico Ferretti, Data Protection and the Legitimate Interest of Data Controllers: Much Ado about Nothing or the winter of Rights? 51 Common Market Law Review (2014); Article 6(f) read with Recital 47, EU GDPR. The 'reasonable interest' formulation is similar to EU GDPR's legitimate interests test with some modifications.

[339] See Data Protection Network, Guidance on the Use of Legitimate Interests under the EU General Data Protection Regulation available at <https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf> (last accessed on 27 March 2018) at p. 10.

[340] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

defeat the purpose of such processing. However, conducting such an anti-fraud exercise would be beneficial for both the data fiduciaries as well as the data principals. Therefore, the company would be justified in proceeding under the ground of 'reasonable purpose'.[341]

(ii) Credit Scoring: A credit card company will share personal data of its customers with credit reference agencies for credit scoring. Here proceeding under 'reasonable purpose' instead of 'consent' may be more appropriate if the credit score of individuals is needed to determine creditworthiness and there is an absence of real choice for the data principals.[342]

Although consent can cover a large gamut of issues, there is a need for a reasonable purpose test in order to cover certain other residuary purposes as listed above.

However, the any freely constituted residuary ground would be too capacious. Its analogous scope in other jurisdictions like the EU demonstrates an inherent lack of standards and uniformity in application, coupled with the possibility of conflict of interests of the data fiduciary.[343] Its existence as a standalone ground for processing appears to be designed to provide latitude to data fiduciaries, without entirely securing the rights of data principals.[344] This may be remedied under the Indian data protection law by circumscribing the ambit of the provision. A list of activities including prevention and detection of unlawful activity like fraud, whistleblowing, mergers and acquisitions, network and information security, credit scoring, and recovery of debt, can be whitelisted by the DPA to guide data fiduciaries. In doing so, the DPA should consider the following factors: the data fiduciary's interest in processing for that purpose, whether it is possible to obtain consent of the data principal, public interest in the processing for that purpose, effect on the rights of the data principal, and the reasonable expectations of the data principal in the context of the processing.

Regardless of the scope of processing, the fundamental rights of data principals should be balanced with the interests of the data fiduciary. This balancing exercise should be done by the DPA in a neutral manner. Further, in order to ensure transparency, data principals should be notified by the data fiduciaries if processing is taking place under this ground.

Processing of personal data made public by a data principal also falls into this category. Conventional views of privacy would offer little protection to such information made public by an individual as the act of making information publicly available could be said to denude the individual of any reasonable expectation of privacy. In the United States, for example,

---

[341] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

[342] UK Information Commissioner's Office, Consultation: GDPR consent guidance available at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (last accessed on 27 March, 2018) at p. 13.

[343] Paolo Balboni et al., Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, 3(4) International Data Privacy Law (2013) at p. 250.

[344] Paolo Balboni et al., Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection, 3(4) International Data Privacy Law (2013) at p. 251.

courts have responded to claims of privacy in such information by developing doctrines such as the "third-party doctrine"[345] or the "plain view doctrine"[346] which grant limited or no protection to information made available to third parties or which is available at a publicly accessible place. The internet provides easily accessible fora including social networking sites where personal data is published or disseminated by data principals. The conventional American approach has been acknowledged to be ill-suited for disclosure of personal data over the internet.[347]

In India, the third-party doctrine has been rejected by the Supreme Court in *District Registrar v. Canara Bank*[348] where the Court noted that documents shared voluntarily with a bank continue to remain confidential vis -à-vis the person, even if they are no longer at the customer's house. This view seems to be closer to the European idea that an individual in spite of any voluntary sharing of, or the disclosure of information would retain an expectation of privacy.[349]

Accepting this approach would also require acknowledging and balancing other societal interests including the rights of third parties. Any strict rule limiting the processing of data made public may impede free speech related to such data on the internet. This problem may be even more significant in the case of public figures where third parties may have a right not only to process personal data made public by the concerned individual but also personal data emanating from other sources including journalistic activities.[350]

On the other hand, limits of fair processing must also be clearly drawn. While an individual making personal data, public may have a lower expectation of privacy, it is unlikely that every kind of disclosure is made with the expectation that personal data may be used for profiling whether by private entities or by the state. In addition to immediate privacy harms to the individual resulting from profiling, leaving personal data made public to be freely subject to data analytics and profiling may have the effect of chilling free speech and social interaction through the use of electronic means. The balancing exercise is further complicated

[345] United States v. Miller, 425 U.S. 435, 442 (1976); this approach is slowly being revisited in the US while recognising that the Fourth Amendment Standards are ill-suited to sharing of information over the internet.
[346] California v. Ciraolo, 476 U.S. 207, 211-12 (1986).
[347] In United States v. Jones, 132 S. Ct. 945, 957 (2012), Sotomayer, J. observed that the approach is "ill-suited to the digital age, in which people reveal a great deal about themselves to third parties in the course of carrying out mundane tasks." See also, Joel Reidenberg, Privacy in Public, 69 University of Miami Law Review (2014).
[348] (2005) 1 SCC 496 (note, however, that this was discussed in relation with questions of confidentiality of data shared with a bank and not strictly in relation with personal data disclosed publicly).
[349] See Case of von Hannover v. Germany [2004], Judgment, European Court of Human Rights (Application no. 59320/00), at paragraph 77: "the Court considers that the public does not have a legitimate interest in knowing where the applicant is and how she behaves generally in her private life even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public"; for a discussion on the difference between the American and European approaches on this point, see Daniel J. Solove and Neil M. Richards, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Georgetown Law Journal (2007).
[350] For further discussion on the processing of data by journalists, see section on journalistic purposes in Chapter 8 of this report; see also, Barrymore v. News Group Newspapers, Ltd. [1997] F.S.R. 600 (Ch.) (U.K.) (discussing issues related to intimate relationships of public personalities) and Florida Star v. BJF, 491 US 524 (1989) (discussing the publication by a newspaper of the name of a rape victim inadvertently disclosed in government records).

by the variety of platforms on the internet. These can range from platforms that permit public disclosures to platforms that facilitate more limited disclosures (such as through a private profile on a social networking site).[351]

It should be noted that the right to be forgotten (discussed in Chapter 5) constitutes a limited response to the problem of personal data available in public. Beyond this, the need for a continuing balancing exercise points to the fact that this processing must be categorised as a reasonable purpose for which the DPA can whitelist permitted actions while maintaining appropriate safeguards.

(c) Application of Obligations

If processing is undertaken under this ground a data fiduciary must comply with all obligations under the data protection law, with the exception of consent, which will not have to be obtained.[352] Further, in the case of activities such as whistleblowing, fraud prevention or routine processing of publicly available data in the exercise of free speech where the obligation to give notice may impede the object of the processing, the DPA may consider exempting the requirement of notice. The DPA is also required to put in place appropriate safeguards or conditions whenever it whitelists a reasonable purpose.

Exemptions

A. White Paper and Public Comments

The White Paper suggested that exemptions may be provided from data processing for household purposes, journalistic/artistic and literary purposes, academic research, statistics and historical purposes, investigation and prosecution of crime, maintenance of national security and public order.[353] Further, it was felt that exemptions should have sufficient safeguards, such as only allowing processing for the stated purpose, while ensuring that they were reasonable and not granted arbitrarily. Further, they should have an effective review mechanism in place.[354]A large number of commenters agreed with the need for exemptions in the law. One commenter suggested limited number of exemptions and avoiding delegated

[351] Such distinctions acknowledge that the legal protection of privacy is not just towards the protection of secrecy but also towards control over the degree of accessibility of data shared. See, for a discussion on this point in relation with the US Freedom of Information Act, Daniel J. Solove, Conceptualizing Privacy, 90(4) California Law Review (2002) at p.1109.

[352] More specifically, the requirements of necessity, proportionality and purpose limitation. See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller (2014).

[353] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 59.

[354] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at p. 59.

legislation as guiding principles in determining exemptions, which would also ensure that the discretionary power of the DPA is restricted.[355]

While a majority of commenters supported an exemption for domestic/personal activities, mixed responses were received on the exemption related to research. Some commenters expressed a view that innovation is an important and legitimate purpose of the state and its subjects. However, there was a general view that the question of balancing this purpose with the right to privacy of individuals is a sensitive call and must be examined in the larger societal and commercial context of research, innovation and advancement.

A number of commenters supported the incorporation of the exemption related to national security. However, a majority of commenters expressed concerns related to roadblocks in implementation, and potential misuse by the state. It was suggested that the text of the legislation must ensure that the exemption in this category is used for a *bona fide* purpose. Further, the law should incorporate strict security safeguards and clearly defined obligations on state agencies. Commenters also highlighted the need for guarding against unfettered state surveillance, and the need for an effective review mechanism and adequate judicial oversight for national security tasks.

B. Analysis

For the creation of a truly free and fair digital economy, it is vital to provide certain exemptions from obligations that will facilitate the unhindered flow of personal data in certain situations. These exemptions derive their necessity from either a state or societal interest. However, these exemptions must be limited to processing that is necessary and proportionate to the purpose sought to be achieved. The data protection law must carefully outline watertight exemptions that are narrow and are availed in limited circumstances. Further, adequate security safeguards must be incorporated in the law to guard against potential misuse. We have identified security of the state;[356] prevention, detection, investigation and prosecution of contraventions of law;[357] processing for the purpose of a legal proceeding; research purposes;[358] personal or domestic purposes; manual processing by small entities; and journalistic purpose[359] as interests which should be privileged with exemptions from certain obligations of the law. As mentioned in the introduction to this chapter, these exemptions will differ in degree and shall operate in a limited manner. The scope and rationale for each of these exemptions is discussed in the relevant sections below.

[355] Comments in response to the White Paper submitted by Supratim Chakraborty, Associate Partner at Khaitan & Co. on 31 January 2018, available on file with the Committee.
[356] *Justice KS Puttaswamy & Anr v. Union of India & Ors* (2017) 10 Scale 1 at page 255 (Chandrachud, J.), at page 38 (Sanjay Kishan Kaul, J.).
[357] *Id* at page 256 (Chandrachud, J.).
[358] *Id* at page 38 (Sanjay Kishan Kaul, J.)
[359] *Id* at page 38 (Sanjay Kishan Kaul, J.) Generally talks about how the right to privacy should be balanced with other fundamental rights.

I. Security of the State

(a) Context

A potent threat to the effectiveness of any data protection framework lies in its permissiveness towards exempting the application of fundamental principles on the grounds of national security. National security is a nebulous term, used in statutes of several jurisdictions to denote intelligence gathering activities that systematically access and use large volumes of personal data.[360] The ostensible purpose of such processing is to continuously gather intelligence to prevent attacks against the country, whether internal or external. Though always an incident of state power, the pervasiveness of such intelligence gathering has significantly expanded in the data economy.[361] It is thus critical to ensure that the pillars of the data protection framework are not shaken by a vague and nebulous national security exception.

It is nobody's case that processing for national security is an illegitimate state interest; it undoubtedly is legitimate, and has been recognised by the Supreme Court of India as such.[362] The key question is what safeguards can be instituted to ensure that the use of this ground is restricted to genuine cases of threats to national security.

The core case for a national security exemption to data protection law arises in the scenario where personal data of targeted individuals is sought in order to prevent a potential threat. It is common sense that in such a case, where information collection and processing requires to be secret and expedited, standard grounds for processing would not apply. Further, since there is no principal-fiduciary relationship in this case, rights of individuals and obligations of entities would be similarly inapplicable. Periodic review alone can ensure that the personal data sought was indeed used for a legitimate national security purpose and not otherwise.

Such a core case however is at odds with how processing of personal data for national security purposes actually works in practice. Contrary to the case-by-case approach on which the core case is premised, intelligence gathering for national security purposes is premised on systematic government access. Systematic government access is understood as direct access by the government to large volumes of personal data held by private sector entities.[363] The

[360] Article 29 Working Party Opinion, Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purpose (2014) available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf> (last accessed on 20 April 2018) at pp. 22-25.

[361] National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law, Directorate General of Internal Policies – Civil Liberties, Justice and Home Affairs, European Parliament (2013) available at <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf> (last accessed on 16 May 2018).

[362] *See Puttaswamy*, (2017) 10 SCALE 1 at page 255 (Chandrachud, J.), at page 38 (Sanjay Kishan Kaul, J.). Further, national security restrictions on rights were upheld in the context of the Terrorist and Disruptive Practices (Prevention) Act, 1987 in *Kartar Singh v. State of Punjab*, (1994) 3 SCC 569 and the Prevention of Terrorism Act, 2002 in People's Union for Civil Liberties (PUCL) v. Union of India, (2004) 9 SCC 580.

[363] See Ira Rubinstein et al, Systematic Government Access to Personal Data: A Comparative Analysis, 4(2) International Data Privacy Law (2014).

revelations by Edward Snowden demonstrated the reality of systematic access by the National Security Agency to personal data held on servers of private companies in the US.[364] However, this is a practice not limited to the US alone — a survey of 13 countries demonstrated its widespread prevalence in the world, including most leading democracies.[365]

In this context, it becomes all the more critical to determine the meaning of the term 'national security'. *Prima facie,* the term itself is alien to Indian constitutional law.[366] Article 19(2), which justifies certain restrictions on freedom of speech and expression, uses the phrase 'security of the State' instead.[367] The Supreme Court has understood this term to mean 'anything tending to overthrow the State'.[368] Certain aggravated instances of public disorder have also been held to affect the security of the state.[369] Further, it has been held to include armed rebellion, leaking information to foreign countries and disaffection in the armed forces, paramilitary or police.[370] Several other statutes use this ground to restrict fundamental rights.[371] It is apparent that what the Constitution understands as 'security of the State' is in common legal parlance today, understood as 'national security'.

In our view, seven decades of jurisprudence provides good reason to adopt the term 'security of the state' in place of 'national security' as an exemption to the fundamental principles of the data protection framework. 'National security' is undefined in every jurisdiction we have studied, and much criticism has been made of this lack of definition.[372] Using 'security of the state' provides greater certainty of which matters can, and cannot, be included as legitimate grounds for exempting the application of data protection principles, based on existing precedent. Further, implicit in this understanding of 'security of the state' is the indication of gravity of the act, as it must be of a nature that tends to overthrow the state itself or affect its security fundamentally. No like indication of gravity is implicit in 'national security' since little jurisprudence has developed.

Having established 'security of the state' as the ground for partial exemption of the data protection law, it is important that certain safeguards to prevent abuse are considered. From the perspective of maintaining the sanctity of the data protection framework, the existing

[364] This systematic access programme is commonly referred to as the PRISM programme.
[365] Such countries include UK, Germany, France and India, see Ira Rubinstein et al, Systematic Government Access to Personal Data: A Comparative Analysis, 4(2) International Data Privacy Law (2014).
[366] There is however the National Security Act, 1980. While it uses the term "national security" in its title and text ("Security of India" in Section 3), it is not relevant to our purpose as it deals only with preventive detention.
[367] Generally, courts have been extremely deferential to the understanding of the executive in its interpretation of a restriction on fundamental rights on the ground of 'security of the state'. See for example, Kartar Singh v. State of Punjab, (1994) 3 SCC 569.
[368] Santokh Singh v. Delhi Administration, 1973 AIR SC 1091.
[369] Brij Bhushan v. State of Delhi, 1950 AIR SC 129.
[370] Union of India v. Tulsiram Patel, 1985 AIR SC 1416.
[371] Section 5, Telegraph Act; and Section 69, IT Act.
[372] "Despite this, most laws simply list 'national security' as a ground for restricting access to information without defining this term at all, let alone providing a specific list of categories of exceptions. In many cases, these laws do not even require the disclosure to pose a risk of harm to national security." Toby Mendel, The Johannesburg Principles: Overview and Implementation available at <https://www.article19.org/data/files/pdfs/publications/jo-burg-principles-overview.pdf> at p. 15; See generally Melvyn P. Leffler, National Security, 77 The Journal of American History (1990).

methods of non-consensual interception and access to personal data in law have to be taken into account and safeguards against misuse scrutinised.

The design of the current legal framework in India is responsible for according a wide remit to intelligence and law enforcement agencies. At the same time, it lacks sufficient legal and procedural safeguards to protect individual civil liberties.[373] Much intelligence-gathering does not happen under the remit of the law, there is little meaningful oversight that is outside the executive, and there is a vacuum in checks and balances to prevent the untrammeled rise of a surveillance society.

There is no general law in India today that authorises non-consensual access to personal data or interception of personal communication for the purposes of intelligence gathering or national security. If there are any entities that are carrying out activities of such a nature without statutory authorisation (for example, solely through executive authorisation), such activities would be illegal as per the *Puttaswamy* judgment as they would not be operating under law. The Intelligence Services (Powers and Regulation) Bill, 2011 had been introduced to regulate the manner of functioning of Indian intelligence agencies and institute an oversight mechanism.[374] However, the Bill lapsed in 2011 and left the legislative vacuum unaddressed.

However, for at least some of the instances of monitoring and interception, access to personal data is currently obtained through certain statutory provisions.[375] For instance, the Telegraph Act authorises interceptions in the interests of the security of the state if the Central Government, State Government or a special officer are satisfied that it is both 'necessary and expedient'.[376] Similarly, under the IT Act, the Central Government may issue directions for monitoring, interception or decryption of information transmitted, received or stored on a computer device, when it is necessary or expedient in the interest of security of the state.[377] Further in the interest of cyber security, the Central Government may authorise an agency to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. All persons must comply with the directions of such authorised agency to avoid imposition of penalty.[378]

[373] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 4.
[374] Manish Tewari, State of the Union: Time for intelligence reforms?, *Deccan Chronicle*, 19 March 2016, available at https://www.deccanchronicle.com/opinion/op-ed/190316/state-of-the-union-time-for-intelligence-reforms.html; See NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 4.

[375] This is not an exhaustive analysis. Other provisions in central and state laws may exist for access for specific purposes. For instance, Section 33, Aadhaar Act permits the disclosure of information by order of a court not inferior to that of a District Judge.
[376] Section 5, Telegraph Act.
[377] Section 69, IT Act.
[378] Section 69B, IT Act.

For each of these mechanisms, oversight is carried out through a Review Committee set up under the Telegraph Rules.[379] This Committee reviews interception orders passed under the Telegraph Act [380] and Section 69B of the IT Act. It consists of the Cabinet Secretary, Secretary to the Government of India in charge of Legal Affairs and the Secretary to the Government of India in charge of Department of Telecommunications. As per a recent RTI application to the Ministry of Home Affairs, it has been found that about 7500-9000 such orders are passed by the Central Government every month.[381] The Review Committee has an unrealistic task of reviewing 15000-18000 interception orders in every meeting, while meeting once in two months.[382]

Additionally, surveillance practices are also enabled by the license agreements entered into by telecom service providers with the Government.[383] For example, such agreements can mandate low encryption standards. This poses a threat to safety and security of the personal data of data principals.

Surveillance should not be carried out without a degree of transparency that can pass the muster of the *Puttaswamy* test of necessity, proportionality and due process.[384] This can take various forms, including information provided to the public, legislative oversight, executive and administrative oversight and judicial oversight.[385] This would ensure scrutiny over the working of such agencies and infuse public accountability.

Executive review alone is not in tandem with comparative models in democratic nations which either provide for legislative oversight, judicial approval or both. Legislative oversight exists in Germany; judicial review in UK; and some form of both in South Africa. At the same time, it is instructive to note that the data protection legislations in each of these countries dovetail with each substantive legislation relating to national security.

Thus, in South Africa, under the Intelligence Services Oversight Act, 1994[386] there is a parliamentary as well as civil oversight mechanism which together hold security structures accountable and receives complaints about intelligence services. Further, the Regulations of

[379] Rule 419A (16), Telegraph Rules.
[380] Section 5(2), Telegraph Act.
[381] Comments in response to the White Paper submitted by Kalyan Biswas, Associate Vice President at Internet and Mobile Association of India on 31 January 2018, available on file with the Committee.
[382] Comments in response to the White Paper submitted by Kalyan Biswas, Associate Vice President at Internet and Mobile Association of India on 31 January 2018, available on file with the Committee.
[383] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 11.
[384] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 21-23.
[385] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 21-23.

[386] The Intelligence Services Oversight Act, 1994, see statement of objects and reasons – "To provide for the establishment of a Committee of Members of Parliament on Intelligence and to define its functions; and for the appointment of Inspectors General or Intelligence and to define their functions; and to provide for matters connected therewith." available at <https://oldsite.issafrica.org/uploads/INTELSERVACT40OF1994.PDF> (last accessed on 19 April 2018).

Interception of Communications and Provision of Communication-related Information Act, 2000[387] requires judicial approval for interception of communication activities. The POPI Act exempts personal data involving national security[388] from its purview to the "the extent that adequate safeguards have been established in legislation for the protection of such personal information."[389]

In Germany, the Parliamentary Control Panel appointed under the Act on the Control of the Intelligence Activities of the Federation, 1978 scrutinises intelligence activities.[390] Comprehensive information on intelligence activities is released to this panel which then reports to the Parliament. Further, administrative control exists in the form of the relevant federal ministries exercising supervision over the intelligence agencies under them and the Federal Commissioner of Data Protection and Freedom of Information who monitor compliance of the federal intelligence agencies with the data protection laws.[391] The Federal Data Protection Act allows for derogation from the data protection law if a public body needs to process personal data "necessary to prevent a substantial threat to public security or necessary for urgent reasons of defence."[392]

In UK, under the Investigatory Powers Act[393] interception warrants can be issued by the Secretary of State upon application by an interception authority which further require approval by the Judicial Commissioner to ensure that the tests of proportionality and necessity were met at the time of issuance of the warrant. The UK DPA exempts personal data required for the purpose of safeguarding national security from the principles of data protection as well as the rights and obligations set out under the law.[394]

In the US, the oversight mechanisms primarily exist in the form of various Congressional committees and mechanisms under the executive office of the President.[395] The House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence

[387] The Regulations of Interception of Communications and Provision of Communication-related Information Act, 2000 available at <https://www.justice.gov.za/legislation/acts/2002-070.pdf> (last accessed on 19 April 2018).
[388] Section 6(1) (c), POPI Act. The term "national security" has been expanded upon as "including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety".
[389] Section 6(1)(c), POPI Act.
[390] Foreign Intelligence Gathering Laws: Germany, Library of Congress available at <https://www.loc.gov/law/help/intelligence-activities/germany.php> (last accessed on 9 May 2018).
[391] Foreign Intelligence Gathering Laws: Germany, Library of Congress available at <https://www.loc.gov/law/help/intelligence-activities/germany.php> (last accessed on 9 May 2018).
[392] Section 22, Federal Data Protection Act. Further, Section 23, Federal Data Protection Act allows for processing of personal data apart from the purpose collected if the data if the "processing is necessary to prevent substantial harm to the common good or a threat to public security, defence or national security".
[393] Section 138, Investigatory Powers Act.
[394] Section 28, UK DPA.
[395] Oversight of the Intelligence Agencies: a comparison of the 'Five Eyes' Nations (2017), Parliamentary Library, Parliament of Australia available at <http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5689436/upload_binary/5689436.pdf>.

are the primary intelligence oversight bodies.[396] Judicial oversight exists under the FISA for *ex ante* judicial approvals for gathering foreign intelligence.[397]

Though each of these jurisdictions provides for external oversight over executive intelligence actions, such mechanisms have been widely criticised as being ineffectual. Thus, in the US, FISA courts have granted 99.97% of all applications.[398] Though by itself this may not determine permissiveness, since, it is argued that the executive may be self-selecting,[399] nonetheless, the acceptance rate is unquestionably high. At the same time, the secret nature of the proceedings means that there is no way of knowing whether the review was indeed fair. Most crucially, judicial approvals for mass intelligence gathering appears to be an example of a category mistake— a form of review more suitable for particularised decision-making being used to authorise systematic access renders remote the possibility of genuine case-by-case approval.

On the other hand, legislative oversight too is subject to considerable criticism. For instance, the Parliamentary Control Panel in Germany has been criticised because its membership solely constitutes of Members of Parliament and they lack the time to study the information in depth.[400] Further, they have no means of verifying the information supplied by the government.[401] Congressional oversight in US has been criticised as being ritualistic and being akin to a 'security theatre' with the vast amounts of information being supplied to the Congress entering a Congressional void.[402]

Despite these criticisms, it is worthwhile to recognise that all the aforementioned jurisdictions provide some form of inter-branch oversight through a statute. Nothing similar exists in India. This is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in *Puttaswamy*, potentially unconstitutional. This is because the Supreme Court has clearly laid down that any restriction of the right to privacy must satisfy three tests: first, the restriction must be by law, second, it must be necessary and proportionate and third, it must promote a legitimate state interest.[403] The salience of procedural safeguards within the interception structure has also been emphasised to prevent abuse. Though the nature of the intelligence gathering in a particular case will have to be carefully scrutinised to ascertain

[396] Oversight of the Intelligence Agencies: a comparison of the 'Five Eyes' Nations (2017), Parliamentary Library, Parliament of Australia available at <http://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5689436/upload_binary/5689436.pdf>.
[397] Sections 103 (a)(1) and 103(b), FISA.
[398] Conor Clarke, Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate, 66 Stanford Law Review Online (2014).
[399] Conor Clarke, Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate, 66 Stanford Law Review Online (2014).
[400] Alvar Freude and Trixy Freude, Echoes of History: Understanding German Data Protection, Bertelsmann Foundation available at <http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/> (last accessed on 9 May 2018).
[401] Alvar Freude and Trixy Freude, Echoes of History: Understanding German Data Protection, Bertelsmann Foundation available at <http://www.bfna.org/research/echos-of-history-understanding-german-data-protection/> (last accessed on 9 May 2018).
[402] See P. M. Schwartz, Reviving Telecommunication Surveillance Law, 75(1) University of Chicago Law Review (2008) at p. 310.
[403] *Puttaswamy*, (2017) 10 SCALE 1 at para 180.

whether it satisfies the second and third tests, several types of current intelligence gathering in India falls at the first threshold, since it is not done under law. Further, statutorily recognised interceptions may also require further scrutiny as to whether they are indeed necessary or proportionate, which are new standards for fundamental rights restrictions to satisfy post *Puttaswamy*.

(b) Scope

It is the Committee's view that the data protection law must contain adequate safeguards to adhere strictly to the judgment of the Supreme Court in *Puttaswamy*. The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is proportionate and necessary in the interest of the security of the state and is pursuant to a law that meets the test of constitutionality. Further, any restriction on privacy must be proportionate and narrowly tailored to the stated purpose. Finally, obligations on maintaining security safeguards in processing personal data will remain on the agency collecting such data and no exemption to the same will be provided.

Following the precedents in other jurisdictions, we also recommend that the Central Government carefully scrutinise the question of oversight of intelligence gathering and expeditiously bring in a law to this effect. Such a law should provide for both parliamentary oversight as well as judicial approval of all requests for non-consensual access to personal data. The key rationale underlying such checks and balances is the need for *ex ante* access control as well as *ex post* accountability. For the former, a district judge may be designated and given security clearance for this purpose in each district to hear such requests and dispose them expeditiously. Given the sensitivity of the matter, such proceedings should be closed-door, with regular reporting to an appropriate parliamentary committee. Further, all such approvals should be time-bound and require renewal on the judge being satisfied that the purpose for processing remains relevant. A periodic review before a parliamentary committee is necessary, where such review should be conducted via closed-door proceedings, as it is done in South Africa.[404] Ex-ante and post-facto reporting and transparency requirements should also be incorporated in the appropriate law.[405]

The surveillance architecture should also embed systematic risk management techniques within itself.[406] This would lead to the prioritisation and narrowing of its activities, by devoting resources to credible risks, whether reputational or organisational.[407] For example, an assessment of whether a particular measure is the least intrusive measure to achieve a

[404] The Joint Standing Committee on Intelligence in South Africa has oversight over all security structures and oversight bodies which must be accountable to it.
[405] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 29.
[406] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.
[407] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

stated aim may be required.[408] Not only will this reduce costs incurred by the State, it will also be consistent with civil rights protection.[409]

We would hasten to add that this recommendation, albeit not directly made a part of the data protection statute, is important for the data protection principles to be implemented effectively and must be urgently considered.

(c) Application of Obligations

Apart from the obligations of security safeguards and fair and reasonable processing none of the other obligations under the data protection law shall apply to the processing of personal data under the security of state exemption. The collection and processing in such situations by its very nature may be covert and expedited, thereby making consent inapplicable. It therefore flows, that obligations such as purpose specification and storage limitation will also not apply through the proposed data protection law and, if applicable, would be implemented in a modified form through the appropriate statute authorising the intelligence activities. Moreover, since a principal-fiduciary relationship has not been envisaged in this case, rights of the individuals will also not be applicable.

II. Prevention, Detection, Investigation and Prosecution of Contraventions of Law

(a) Context

Prevention, detection, investigation and prosecution of contraventions of law (including disciplinary proceedings and investigation into tax contraventions) are important state functions, central to the protection of individuals and the society at large. It is a legitimate aim of the state.[410] The state enjoys a monopoly of the legitimate use of physical force to enforce order within its sovereign territory.[411] The Constitution entrusts State Governments and Union Territories with the maintenance of law and order,[412] including "prevention, detection, registration, investigation and prosecution of crimes."[413] While these activities are in pursuance of a legitimate aim of the state, they must meet the test of necessity and proportionality, as laid down in *Puttaswamy*.[414]

Law enforcement activities stem from the larger obligations of the state to maintain public order in society. The Committee acknowledges that sometimes the line between situations

[408] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.
[409] NIPFP Technology Policy, Use of personal data by intelligence and law enforcement agencies, June 27, 2018, p. 28.

[410] *Puttaswamy*, (2017) 10 SCALE 1, Part S, para 181.
[411] H.H. Gerth and C. Wright Mills (eds.), Max Weber: Essays in Sociology (Oxford University Press, 1946).
[412] Entry 1 and 2, List II, Schedule VII, Constitution of India.
[413] Response of the Minister of Home Affairs (Government of India) to unstarred question no. 1354 (Lok Sabha) (5 March 2013) available at <https://mha.gov.in/MHA1/Par2017/pdfs/par2013-pdfs/ls-050313/LSQ.1354.Eng.pdf > (last accessed on 10 May 2018).
[414] *Puttaswamy*, (2017) 10 SCALE 1.

threatening the security of state and those posing a threat to public order may be blurred.[415] Since law enforcement agencies are also engaged in anticipating and preventing possible attacks, it may become difficult to ascertain when a disorder will constitute a mere crime and when it may transcend to a threat to national security. The term "public order" has been understood to mean less aggravated forms of disorder that disturb public peace and tranquillity in comparison to endangering the "security of state".[416] Accordingly, the data protection law should distinguish between exemptions provided for the purpose of national security and law enforcement.

The focus of law enforcement activities of police, investigating authorities and revenue authorities is on individuals. Consequently, a significant amount of personal data is processed while undertaking these activities. Courts in India have often had to resolve the continuous conflict between issues of spatial and informational privacy, liberty and autonomy of the individuals, while ensuring safety of citizens through law enforcement.[417] In this context, it is critical for a data protection law to effectively address concerns relating to the right to privacy of individuals, and at the same time ensure that crucial state functions are not impeded. Data protection laws across jurisdictions have carved out specific exemptions for processing related to prevention, detection, investigation and prosecution of contraventions of law.[418]

As per the RTI Act, information which would impede the process of "investigation or apprehension or prosecution of offenders" is exempted from being disclosed to any citizen.[419] The phrase has been interpreted to include investigation during disciplinary proceedings, investigation by income tax authorities, etc. While there is no watertight definition of the terms "investigation" or "prevention and detection of crime", a perusal of criminal legislation in India lends sufficient clarity. The CrPC provides an inclusive definition of the term 'investigation' to mean all proceedings under the CrPC for the "collection of evidence conducted by a Police officer or by a person (other than a Magistrate) who is authorised by a Magistrate in this behalf".[420]

The procedural aspects regarding the recording of crimes, investigation of criminal cases and execution of arrest, search and seizure are dealt with under the CrPC. It contains detailed provisions on arrest to stipulate when a police officer can make an arrest without a warrant[421] or on refusal to furnish name and address,[422] arrest by private person,[423] arrest by

[415] It is relevant to note the theory of "three concentric circles", i.e. "law and order" (largest), "public order" and "security of state" (smallest), as discussed in Ram Manohar Lohia v. State of Bihar, AIR 1966 SC 740.
[416] Romesh Thapar v. State of Madras, AIR 1950 SC 124.
[417] Directorate of Revenue v. Mohammad Nisar Holia, (2008) 2 SCC 370 at para 14; People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC at para 18; ITO v. Seth Bros., (1969) 2 SCC 324 at para 8; Bai Radha v. State of Gujarat, (1969) 1 SCC 43 at para 10.
[418] See Section 29, UK DPA; Clauses 31 and 43(3), UK Data Protection Bill; Section 6(1)(c)(ii), Sections 15(3)(c)(i), 18(4)(c)(i), 22(3), 37(2)(b), POPI Act.
[419] Section 8(1) h, RTI Act.
[420] Section 4(h), CrPC.
[421] Section 41, CrPC.
[422] Section 42, CrPC.

Magistrate[424] etc., as well as how such arrest should be made.[425] Under Section 91 of the CrPC, an officer in charge of a police station can require a person, by written order, to produce a document or any other thing that is "necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Code". As per the CrPC, an investigation may also include the ascertainment of facts and circumstances of a case, search and arrest of a suspected offender, search of the premises and seizure of material important to the investigation, examination of various individuals relevant to the case etc.[426] In all these stages, personal data is processed by the police.

The PMLA grants powers of search and seizure to an authorised officer.[427] Here, the authorised officer may seize any record or property found during the course of search, and retain the seized property or record if the retention is necessary for an inquiry.[428] The NIA Act is geared towards curbing terror attacks, militancy and insurgency. It provides wide powers to investigate connected offences along with scheduled offences.[429] Further, apart from police investigations, regulators like the SEBI and the CCI grant powers to investigating authorities to search places,[430] seize books, registers, documents and records,[431] keep such information in custody,[432] conduct inquiries into alleged contravention of the applicable law,[433] and conduct inquiries into disclosures made.[434]

The Income Tax Act also provides powers to the state authorities to make enquiries or investigate whether income has been concealed towards the protection of revenue.[435] Their powers of enquiry and investigation also extend to any persons or class of persons in relation to an agreement entered into by the Central Government with a territory outside India,[436] as specified under the Income Tax Act. Further, authorities under the Income Tax Act also have powers to conduct raids,[437] search and seizure,[438] call for information,[439] etc. Disclosure of an assessee's information may be made to other authorised officials of the Central Government if it is necessary in public interest.[440] In these instances, tax authorities are compelled to process personal data in compliance with law.

---

[423] Section 43, CrPC.
[424] Section 44, CrPC.
[425] Section 46, CrPC.
[426] H.N. Rishbud v. State of Delhi, 1955 AIR SC 196.
[427] Section 17, PMLA.
[428] Section 20 and 21, PMLA.
[429] Section 8, NIA Act.
[430] Section 11C, SEBI Act.
[431] Section 11C, SEBI Act.
[432] Section 11C, SEBI Act.
[433] Section 19, Competition Act.
[434] Section 30, Competition Act.
[435] Section 131, Income Tax Act, 1961
[436] Sections 90 and 90A, the Income Tax Act.
[437] Section 132A, Income Tax Act.
[438] Section 132A, Income Tax Act.
[439] Section 133, Income Tax Act.
[440] Section 138, Income Tax Act.

Activities in furtherance of prevention, detection, investigation and prosecution of contraventions of law carried out by law enforcement and revenue agencies may involve processing of personal data as well as sensitive personal data, including DNA samples, biometrics, and official identification documents. Further, advancements in technology have led to significant changes in data collection methods adopted. Given the wide range of powers that law enforcement and revenue agencies enjoy when working towards the prevention, detection, investigation and prosecution of contraventions of law, it is important to verify whether sufficient checks exist on such powers to ensure that they would not unlawfully impinge on the data protection rights of the individuals whose data gets processed in the course of such investigations.

In India, these agencies are subject to parliamentary, executive and judicial oversight as well as scrutiny by other independent statutory bodies.[441]

Further, several independent authorities also oversee the functioning of law enforcement agencies to prevent and counteract any abuse of power. For example, the CVC is authorised to receive complaints for and investigate corruption, malpractice or misuse of office allegations.[442] The CAG audits the accounts of investigatory authorities and therefore checks against the misappropriation of funds.[443] The National Human Rights Commission, though without any binding powers, also possesses the authority to probe into alleged human rights violations by the police.[444] Some states also have a body called the Police Complaints Authority where persons can lodge complaints of 'serious misconduct' against the police.[445]

---

[441] The Parliament through its select committees and department related standing committees periodically reviews laws which provide such powers to law enforcement agencies. See Mario J. Aguja and Hans Born (eds.) DCAF, The Role of Parliament in Police Governance (2017) available at <https://www.dcaf.ch/sites/default/files/publications/documents/The_Role_of_Parliament_in_Police_Governance.pdf> (last accessed on 10 May 2018). The Executive exercises control over such agencies through the Ministry of Home Affairs which is responsible for all central police forces as well as the Indian Police Service. The Home Minister is also accountable to the Parliament and the relevant State Legislatures. At the local level, the Superintendent of Police is empowered to initiate an inquiry into any complaint made against a subordinate officer. Further, the police force at the district level is placed under the control of the District Magistrates, who also have the power to give guidance to the police (Section 4, Police Act, 1861).
Indian courts have also been proactive in upholding the human rights of Indian citizens against abuses by the police. The Supreme Court, for instance, has come out with guidelines to ensure better accountability for the police and has delivered judgments punishing the police for not following due process or for the abuse of their power (Centre for Law and Policy Research, Legal Accountability of the Police in India (2016) available at <http://clpr.org.in/wp-content/uploads/2016/08/140214-Police-Accountability-website.pdf> (last accessed on 10 May 2018). In the case of *Prakash Singh* v. *Union of India* ((2006) 8 SCC 1), the Supreme Court laid down several means of checks and balances on the powers of the police which included the constitution of State Security Commissions, Police Establishment Boards and Police Complaints Authorities. The Supreme Court had also directed that the investigation wing of the police be separated from the law and order wing to improve investigation time and expertise and further recommended the setting out of a minimum tenure for key police officers. Further, another mechanism of ensuring that the law enforcement agencies do not process personal data that is not strictly necessary for investigation, is by requiring them to obtain search warrants from judicial magistrates (Section 93 CrPC).

[442] Section 8, Central Vigilance Commission Act, 2003.

[443] The powers and functions of the CAG have been laid down in the Comptroller and Auditor General's (Duties, Powers and Conditions of Service) Amendment Act, 1971.

[444] Mario J. Aguja and Hans Born (eds.) DCAF, The Role of Parliament in Police Governance (2017) available at

Despite these safeguards, it is critical that the principles laid down in the *Puttaswamy* judgment regarding the use of personal data for law enforcement pursuant to a legitimate aim of the state, applied in a necessary and proportionate manner by law need to be followed strictly. The details of application of the principles are contained in (c) below.

(b) Scope

The Committee is of the opinion that the data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law for both personal as well as sensitive personal data. For this purpose, the specific law enforcement authorities which can claim the use of this exemption would also have to be limited by the data protection law to ensure that there is no scope for the exploitation of vagueness in the law. Further, while the rationale for the provision of this exemption is the maintenance of public order, the term public order must be constrained by specific activities aimed at prevention, detection, investigation and prosecution of crimes, which are constitutional and statutorily derived.

Generally, laws in India grant investigating authorities and the police significant powers to process personal data of individuals. These individuals may be suspects, witnesses, informants, accomplices, victims, offenders and so on. Therefore, personal data of individuals who are not suspected of, or linked to, a crime being investigated should be permitted to be processed only when absolutely necessary for a legitimate and well-defined purpose and only for a limited period of time.[446]

Further, sensitive personal data, should only be processed when strictly necessary for the purposes of a particular inquiry. When processing does take place for such purposes, the data protection law should subject the data fiduciary to more rigorous standards of obligations of security and accuracy. Even within the category of sensitive personal data, which are capable of causing great harm particularly due to their immutable nature, and capacity to automatically identify individuals, should be subject to a greater degree of oversight before their collection.[447]

<https://www.dcaf.ch/sites/default/files/publications/documents/The_Role_of_Parliament_in_Police_Governance.pdf> (last accessed on 10 May 2018).

[445] To maintain independence, such a body is to consist of a retired high court judge, and may consist of retired senior level police officer or civil servant. Centre for Law and Policy Research, Legal Accountability of the Police in India (2016) available at <http://clpr.org.in/wp-content/uploads/2016/08/140214-Police-Accountability-website.pdf> (last accessed on 10 May 2018).

[446] Article 29 Working Party Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive (2013) available at <http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2013/wp201_en.pdf> (last accessed on 10 May 2018).

[447] Article 29 Working Party Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (2015) available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp233_en.pdf> (last accessed on 10 May 2018).

To avail this exemption with regard to investigation into tax contraventions, processing activities must be carried out strictly in accordance with the relevant statutory provision and the state agency should comply with the obligations and safeguards provided in the statute itself.[448]

(c) Application of Obligations

In instances where law enforcement activities are *bona fide*, and are in pursuance of a legitimate state aim as authorised by law, strict adherence to data protection obligations such as giving privacy notices, providing data principal rights, limiting the use of such data to a particular purpose would impede the purposes sought to be achieved. However, the Committee also recognises that an overbroad exemption in this category may amount to an unreasonable restriction on an individual's right to privacy in certain cases and could defeat the overall objective of a data protection law.

Accordingly, the data protection law should require law enforcement agencies to ensure that processing of personal data is necessary and proportionate to their purposes. For instance, maintenance of a DNA database of all citizens, some of whom may be innocent, to track crime, without legal sanction, would be a disproportionate law enforcement measure. A similar exercise was undertaken in the UK[449] where subsequently, the government had to delete more than a million records of innocent adults and children after the enactment of the Protection of Freedoms Act, 2012 which *inter alia* regulates the collection, retention, destruction of biometric data, surveillance mechanisms etc.[450]

In most instances, it will be difficult for law enforcement authorities to comply with strict standards of purpose specification. This is because the very nature of investigation is such that the investigator is unaware of the exact manner in which the investigation would be concluded, and subsequently the result of such investigation. Therefore, purpose limitation would not apply where processing of personal data under this exemption is carried out for the prevention, detection, investigation and prosecution of contraventions of law. Whereas purposes may be largely unclear when contraventions are to be prevented or detected (e.g. CCTV surveillance), investigations would still have purposes in a broad sense insofar as the relevant contravention is largely understood. However, this may not meet the standards of purpose specification in the law.

Personal data would however only be collected for the purposes of prevention, detection, investigation and prosecution of contraventions of law. For instance, the local police may

[448] On the powers of Revenue Officers under Section 132 (Search and Seizure) of the Income Tax Act; ITO v. Seth Brothers, 1969 (2) SCC 324 at para 8.

[449] Peter M Schneider and Peter D Martin, Criminal DNA Databases: the European Situation, 119 Forensic Science International (2001) at p. 232.

[450] National DNA Database of UK; see Sujatha Byravan, The Problems with a DNA Registry, The Hindu (8 May 2018) available at <http://www.thehindu.com/opinion/op-ed/the-problems-with-a-dna-registry/article23805145.ece> (last accessed on 10 May 2018); see also Margarita Guillén et al, Ethical-Legal Problems of DNA Databases in Criminal Investigation, 26 (4) Journal of Medical Ethics (2000).

collect the name, phone number, and address of the victim and the accused. Seeking information about their religion, caste or tribe may not be relevant to the investigation. However, in order to make a case for collecting information such as their biometrics, the police would be required to ensure that such collection is necessary and proportional to the purpose of investigation.

The obligations of notice and consent ordinarily imposed on data fiduciaries would adversely affect the operation of law enforcement agencies because the coercive powers of these agencies, which may at times impinge on individuals' privacy, are necessary to allow the lawful access to information which would be otherwise unavailable to them. Further, it could lead to problems in obtaining evidence and testimonies from witnesses and may also impede the flow of information between different criminal intelligence agencies.[451] Similarly, providing data principal rights such as access, confirmation, correction, portability and the right to be forgotten would be prejudicial to the law enforcement purpose since it may be necessary to prevent and detect crimes that the suspect is not made aware of an investigation running against him for fear of destruction of evidence.

Processing for investigation into tax contraventions should be exempt from the obligations related to notice, consent, use, and disclosure. This is because compliance with these obligations may defeat the purpose of the statutory provision under which such processing is being carried out. For instance, seeking consent of an individual before conducting search and seizure under the Income Tax Act to ascertain whether there has been a tax evasion, may jeopardise the object of conducting such raids. Similarly, the provision on data principal rights as set out in the data protection law will not apply. In certain instances, personal data may be accessed or rectified subject to the statutory provisions set out in the respective tax and revenue legislation. The obligation of maintenance of security safeguards to ensure safety and integrity of citizens' data should be applicable to officials and authorities discharging such functions.

III. Processing for the purpose of legal proceedings

(a) Context

Non-disclosure provisions in the data protection law will be inapplicable to disclosure of personal data necessary for enforcing any legal right or claim, for seeking any relief, defending any charge, opposing any claim, or obtaining legal advice from an advocate in an impending legal proceeding.

The rationale for exempting the disclosure of personal data in the pursuance of legal claims is to allow data principals to effectively exercise their legal rights under general law, including

[451] See Chapter 37: Agencies with Law Enforcement Functions, Australian Privacy Law and Practice (ALRC Report 108).

the ability to take legal advice from advocates. Applying the obligations under the proposed data protection law may obstruct the realisation of such rights.

Further, processing of personal data by any court or tribunal in India necessary for the exercise of any judicial function will be exempted. This is to cover instances of processing by courts in the performance of their judicial function of resolving disputes brought before it.

(b) Scope

Under the Indian data protection law, disclosure of personal data and sensitive personal data in pursuance of a legal claim would occur if it is required to be produced in connection with any legal proceeding (including in preparation for a legal proceeding to be initiated in the future), or where required to establish, exercise or defend legal rights; or where it is required to be brought to the attention of an advocate for seeking legal advice for an impending legal proceeding. Additionally, processing of personal data by any court or tribunal necessary for the exercise of judicial function shall be exempted.

(c) Application of Obligations

For both disclosure of personal data in pursuance of legal claims and seeking legal advice, as well as processing by any court or tribunal in India for the exercise of any judicial function, the data protection obligations of consent, notice, data principal rights and accuracy will not apply as they may hamper the meaningful exercise of legal rights. However, general obligations with regard to security safeguards and fair and reasonable processing will continue to apply.

IV. Research Activities

(a) Context

The Constitution recognises the development of scientific temper, humanism and the spirit of inquiry and reform as one of the fundamental duties of every Indian citizen. [452] In order to facilitate this, an exemption for purposes of research has been considered necessary by the Committee to allow for scientific innovation and free flow of ideas and information. In the context of data protection, the need for this exemption arises because certain principles of data protection such as consent, purpose specification, storage limitation and certain data principal rights may not apply, may be at odds with the achievement of research purpose or may prove to be too onerous to fulfil. While in a completely different setting, such exemptions have existed in Indian law in the form of the research exemption in patent law,[453] which allows for the uninhibited use of patented articles or processes for research and

[452] Article 51A (h), Constitution of India.
[453] Section 47, Indian Patent Act, 1970.

experimentation.[454] The intention behind such exemption is to encourage scientific temper and ensure that larger societal interests, such as innovation and spread of knowledge continue without being unduly restricted.[455]

Moreover, such an exemption also operates in pursuance of the constitutional right to free speech and expression.[456] This is especially true in the context of historical research, where the fundamental right to express oneself may be restricted by rights such as the right to be forgotten, since the epochal quality of information may only become clear long after its creation.[457] The social good in the exercise of such rights is undeniable since they contribute to the free flow of information and ideas in society.

In academic literature, however, research activities are often viewed in contradistinction to an individual's right to privacy which a data protection law seeks to protect.[458] In our view, as Valerie Steeves argues, such a formulation is problematic since data protection helps build trust in research practices, mitigates the commercial imperatives that flow from the fact that research is often a public-private enterprise and protect the accuracy of data.[459] Thus in our approach, research activities and data protection are not viewed as a zero-sum game, but as being complementary to each other.

(b) Scope

In the context of data protection, subject to safeguards, in some form or the other, exemptions for archival purposes in public interest, historical, scientific, and statistical research exist in various jurisdictions.[460] While this formulation is common, it is important to understand the ambit of these terms in order to justify their exemption from data protection law. The EU GDPR provides guidance on the meaning of these terms. Archival services are understood as being in pursuance of a law that provides the legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest.[461] Scientific research is understood in a broad manner, including technological development and demonstration, fundamental research, applied research, privately funded research and research conducted in the area of public

[454] For further details, see K. Chakravarthy and N. Pendsey, Research Exemptions in Patent Law, 9 Journal of Intellectual Property Rights (2004) at pp. 332-341.
[455] *Puttaswamy*, (2017) 10 SCALE 1 at part T, para 5, recognised innovation and spread of knowledge has been recognised as a legitimate concern of the State.
[456] Article 19(1)(a), Constitution of India.
[457] A. D. Baets, A Historian's View on the Right to be Forgotten, 30 International Review of Law, Computers and Technology (2016) at pp. 57-66.
[458] For instance, see M. Mostert et al., Big Data In Medical Research And Eu Data Protection Law: Challenges to the Consent or Anonymise Approach, 24(7) Journal of Human Genetics (2016); J. Tu et al., Impracticability of Informed Consent in the Registry of the Canadian Stroke Network, 350(14) New England Journal of Medicine (2004) at pp. 1414–1422.
[459] See Valerie Steeves, Data Protection and the Promotion of Health Research, 2(3) Healthcare Policy (2007) at pp. 26-38.
[460] Examples include South Africa (Section 27(1)(d), POPI Act), EU (Article 5(1) and Article 89, EU GDPR) and the UK (Section, 33 DPA).
[461] Recital 158, EU GDPR.

health.[462] Historical research, while not explicitly defined is understood to include research for genealogical purposes.[463] Statistical research means any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results with these results capable of being used for different purposes including scientific purposes.[464]

The underlying theme across these categories and the manner in which they have been defined is the advancement of knowledge in public interest. Our law would extend the exemption to research, archival and statistical purposes due to this aspect inherent in each of these activities, since the meaning of the term research is well understood.

(c) Application of Obligations

The research exemption is not being envisaged as a blanket exemption. Only those obligations should be exempted where it is necessary to achieve the object of the research in public interest. Cases in which obligations may have to be exempted are however contextual and dependent on the nature of the research. Thus for instance, while consent and notice requirements may be a *sine qua non* in most forms of medical research such as clinical trials, requirements of informed and opt-in consent may be not be appropriate models for large scale population health research where non-participation may introduce bias thereby influencing the accuracy of the results.[465] Even research processing that is not intended to identify particular persons would be hit by the law if the research data contains enough features to inadvertently allow for such identification.

Purpose specification, which requires the data fiduciary to process for a specific purpose that must be known at the time of collection, may similarly not apply in cases where overwhelming amounts of data. While not collected for research purposes, these may possess the potential to gain research value afterwards.[466] Similarly data storage obligations that require data to be retained as long as retention is necessary to achieve the purpose of processing may not apply since it can inhibit potential research opportunities. It is difficult to always predict the various ways in which a dataset can be used by researchers in the future.[467]

Data principal rights such as access, confirmation and correction may sometimes prove to be onerous to comply with by research organisations processing such data since they may not have the resources to ensure effective compliance. Moreover, exercise of rights such as right

[462] Rectal 159, EU GDPR.
[463] Recital 160, EU GDPR.
[464] Recital 162, EU GDPR.
[465] See Chapter 64: Research, Australian Privacy Law and Practice (ALRC Report 108).
[466] A. D. Baets, A historian's view on the right to be forgotten, Vol. 30 International Review of Law, Computers and Technology (2016).
[467] Ateneo De Manila University, Philippines, Is Research Exempt From Data Protection? available at <https://www.ateneo.edu/udpo/article/Is_research_exempt_from_data_protection> (last accessed on 2 May 2018).

to be forgotten may prove inherently detrimental to historical research or other research based on longitudinal data.[468]

However, since the exemption of obligations will be highly context specific it is difficult to lay down a bright line test that exhaustively provides for which obligations will be exempted in what circumstances. In fact, laying down requirements in the law may result in too broad an exemption for categories such as sensitive medical research where standards like consent should otherwise be the norm.[469] Hence, the DPA will have the authority to exempt the operation of obligations if they effectively preclude the achievement of the research purpose. Further, the DPA may also exempt the operations of obligations if compliance will disproportionately divert resources from the achievement of the research purpose.

Safeguards with regard to processing for research purposes are however essential to ensure that the research exemption is not misused. Processing under the exemption would thus be conditional on the processing of data not supporting decisions with respect to individuals[470] or the processing creating a risk of significant harm to individuals. The operation of the various exemptions for research purpose would therefore be subject to these conditions at all times. Further, measures such as de-identification should also be undertaken where the research can still be carried out under such conditions. It is also necessary to ensure that data is not processed in a manner that supports targeted actions with regard to individuals. Obligations such as data security that require the implementation of technical and organisational measures to ensure the confidentiality, integrity and accessibility of data will continue to apply. Lastly, any applicable codes of ethics with regard to processing of special categories of research such as medical research will in any case have to be complied with at all times.

V. Personal or Domestic Purposes

(a) Context

Processing activities of an individual which are insignificant and are carried out for a purely personal or domestic purpose are usually placed outside the scope of a data protection law. This is because such processing is considered necessary for the development of the individual and cultivation of social relationships. For instance, where an individual has used a camera to take photographs and record videos of surroundings while on vacation, even though this would include personal data of persons captured on camera, the personal exemption would apply as it relates to an individual's personal activity for the cultivation of social relationships and role as a member of society. For these reasons, data protection laws across jurisdictions

[468] Ateneo De Manila University, Philippines, Is Research Exempt From Data Protection? available at <https://www.ateneo.edu/udpo/article/Is_research_exempt_from_data_protection> (last accessed on 2 May 2018).
[469] The broad nature of research exemption under the EU GDPR has in fact been criticised as being detrimental to the interests of individuals especially in the context of genetic research, see K. Pormeister, Genetic Data and the Research Exemption: Is The GDPR Going Too Far?, 7(2) International Data Privacy Law (2017).
[470] Such conditions have been imposed by Section 33, UK DPA in the context of the research exemption.

have had little involvement with private citizens processing their personal data for a domestic purpose.[471]

The key question that arises in this context is what is meant by 'personal'. As per the Court of Justice of the EU's decision in *Bodil Lindqvist*,[472] if personal data disseminated on the internet is accessible to an indefinite number of people, then such dissemination would not qualify as personal or domestic processing as the purpose ceases to remain 'purely personal'.

Further, several data protection legislation exempt personal data processed by natural persons "in the course of a purely personal or household activity".[473] An implicit distinction has been drawn between purely personal activity having no professional or commercial nexus, and personal activity bearing such nexus. For example, personal views about friends expressed on a private social media account would be exempt under this provision, as it is a purely personal activity. However, views expressed on a public social media profile by employees of an organisation may not be exempt. This is because there is a commercial nexus to the activity as it is in the context of the activities of a commercial venture.

As the scope of activities that may be considered 'personal' widens, the possibility of conflating the personal or domestic exemption with other exemptions may increase. For example, an individual's personal blog may qualify for both the personal and journalistic exemptions, depending on the nature of the content, the frequency and scale at which the content is disseminated, the nature of the blog etc.

The widespread use of social networking services leads to a similar conflation.[474] Access to the internet has enabled individuals to disseminate information quickly and widely, an ability formerly restricted to media and publishing organisations.[475] Users exercise control over the information that they disclose online, which often contains personal data related to them. In some cases, information shared by such individuals may also include personal data related to

---

[471] Proposals for Amendments regarding exemption for personal or household activities available at <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf > (last accessed on 12 April 2018).

[472] Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01.

[473] Article 2(2)(c), EU GDPR; Section 36, UK DPA; Art. 2(2)(a); Section 5(3), Personal Data Protection Code, 2003, Italy. See also Recital 18, EU GDPR provides: "this Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities."

[474] Rebecca Wong, Social Networking: a Conceptual Analysis of a Data Controller, 14(5) Communications Law (2009).

[475] Rebecca Wong, Social Networking: a Conceptual Analysis of a Data Controller, 14(5) Communications Law (2009). See also Article 29 Working Party, Opinion on Data Protection Issues Related to Search Engines, available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf> (2008); UK Information Commissioner's Office, Social networking and online forums- when does the DPA apply? available at <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2013/06/UK-ICOsocial-networking-and-online-forums-dpa-guidance.pdf> (last accessed on 3 May 2018).

their friends and family, or other individuals (for example, tagging strangers or third parties in photographs without their consent). Such disclosure may be made to a restricted friend list or to the public at large. In such cases, the application of the personal/domestic exemption would depend on the nature of the post. For instance, as per the principles laid down in *Lindqvist*,[476] even a private social media post containing personal data of individuals other than the user may not be covered by the personal exemption depending on the facts of the case. The individual here would be a data fiduciary.

Similarly, a domestic CCTV installed in an individual's residential premises which captures the video of strangers cannot be regarded as strictly personal. In *František Ryneš*,[477] the Court of Justice of the EU held that the image of a person recorded by a camera qualifies as personal data. The Court opined that a security camera system installed by an individual in her home which simultaneously monitors a public space does not qualify as purely personal or domestic activity.

(b) Scope

The Committee recognises that activities carried out by individuals for a private purpose, or in fulfilment of a daily domestic task requires protection. Therefore, a narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. If an act of processing falls within this category, the obligations and rights under the law will not apply as such application would be disproportionate, impracticable and onerous on the individual. In other words, processing of both personal and sensitive personal data carried out for a personal or domestic purpose would enjoy a blanket exemption from the application of the data protection law.

(c) Application of Obligations

The Committee acknowledges that the absolute nature of this exemption means that the determination of whether an activity is purely personal or domestic will be paramount. Therefore, an activity would not be considered purely personal or domestic if such processing involves any public disclosure, or if it involves any professional or commercial activity. The exemption would not apply in these cases. In the EU, certain guidelines have been laid down to ascertain whether an act of processing is personal, such as the number of people the personal data is being disseminated to, whether the personal data is about individuals who are not personally related to the individual posting it, scale and frequency of processing, potential harm, and whether it is partly personal and partly professional.[478] If processing falls outside

[476] Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01

[477] František Ryneš v. Úřad pro ochranu osobních údajů, Case C212/13, 11 December 2014; See also Lindqvist v. Åklagarkammaren i Jönköping, Case C-101/01.

[478] Proposals for Amendments regarding exemption for personal or household activities available at <http://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf> (last accessed on 12 April 2018); Lindqvist v Åklagarkammaren i Jönköping, Case C-101/01.

of this ambit, the data protection law will continue to apply.[479] Similar guidelines may evolve in the Indian context through case laws over the course of time. This provision would ensure that the law does not become onerous for private individuals, as well as prevent misuse by individuals for professional or commercial gains.

VI. Journalistic Activities

(a) Context

(i) Conflict between Privacy and Free Speech

A good data protection law needs to achieve a balance between competing social interests. One such conflict exists between the right to free flow of information through freedom of speech and expression and the right to restrict such flow in the interest of privacy and safeguarding of the handling of personal data.

Freedom of expression is necessary to ensure a participatory democracy where citizens have free and fair access to information. Given the large volume of information and the multiple sources such information originates from, journalists and media houses act as the conduit to relay such information in an accessible manner. The role of a journalist is to be 'an analyst and interpreter of the events'[480] and to serve as 'proxy witnesses and information-gatherers'.[481] Journalism acts in public benefit since it helps in building social accountability and brings about discussions on issues of public concern.[482] If journalists were made to adhere to the grounds of processing personal data, it would be extremely onerous for them to access information. Further, mandating grounds of processing like consent would mean that accounts that are unfavourable to the data principal would simply not get published. There therefore exists a public interest in the untrammelled dissemination of news, current affairs and documentaries, especially when they inform, criticise and analyse issues of public importance. However, it could be argued that even material apart from the above may be relevant to the general interests of the public and the flow of such information should not be impeded.

---

[479] See The Law Society and Others v. Rick Kordowski (Solicitors from Hell), [2011] EWHC 3185 (QB) where the individual was held to be a data controller.

[480] Donald H. Johnston, Journalism and the Media (1979) at p. 108 as cited in Jonathan Peters and Edson C. Tandoc, Jr., People Who Aren't Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[481] Judith Clarke, How Journalists Judge the 'Reality' of an International 'Pseudo-Event', 4 Journalism (2003) as cited in Jonathan Peters and Edson C. Tandoc, Jr., People Who Aren't Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[482] William F. Woo, Defining a Journalist's Function, 59 Nieman Reps (2005) at p. 33 as cited in Jonathan Peters and Edson C. Tandoc, Jr., People Who Aren't Really Reporters At All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

At the same time, as has been stressed throughout this report, the fundamental right to privacy encompasses within itself the protection of personal data of individuals and therefore, needs protection. The Supreme Court of India, in the case of *R. Rajagopal* v. *State of Tamil Nadu*[483] has held that citizens have the right to protect their privacy and the publication of personal information without consent regardless of the nature of content of such publication may violate the privacy of the person concerned.

To be able to give effect to both these rights, it is essential to ensure a balance between the freedom of expression and the safeguarding of personal data for the public good of a free and fair digital economy. This can be done by allowing recourse to the journalistic exemption where public interest in the disclosure of the personal data is overriding. Here it becomes important to determine what public interest means. The standard for determining whether the published material violates the concerned individual's privacy would be that of a reasonable person and not that of a hyper sensitive person.[484] It has also been held that public interest has to be more than mere idle curiosity. The balance between freedom of expression and privacy has to be struck by considering factors such as the interest of the community and the proportionality of protecting one right against the infraction of the other.[485] In the US, a standard of newsworthiness is used instead where the term would include material which could be 'fairly considered as relating to any matter of political, social, or other concern to the community' or when it 'is a subject of general interest and of value and concern to the public.'[486] The threshold for what counts as public interest is understandably low and vague,[487] although, the Indian judiciary has laid down factors like likelihood of injustice, sensitivity of the relevant information, passage of time and class of persons affected to broadly draw out a scope for the term.[488]

To be able to strike a balance between the aforementioned rights and be able to ascertain when one right should constrain the other, it is important to first be guided by what would best serve public interest. Second, the broad contours of what journalism and a journalist would signify should also be laid down. Finally, it is essential to ensure that journalists do not abuse the rights of the data principals by mandating that they are committed to upholding certain standards of privacy which are coterminous with the data protection law.

---

[483] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[484] Ajay Goswami v. Union of India, (2007) 1 SCC 143.
[485] Indu Jain v. Forbes Incorporated, (2007) ILR 8 Delhi 9.
[486] Snyder v. Phelps, 562 U.S. 443 (2011).
[487] Bihar Public Service Commission v. Saiyed Hussain Abbas Rizwi, (2012) 13 SCC 61 held "The expression "public interest", like "public purpose", is not capable of any precise definition. It does not have a rigid meaning, is elastic and takes its colour from the statute in which it occurs, the concept varying with time and state of society and its needs." The Black's Law Dictionary defines it as the general welfare of the public that warrants recognition and protection; something in which the public as a whole has a stake."
[488] R.K. Jain v. Union of India, (1993) 4 SCC 120 held that "the factors to decide public interest would include, "(a) where the contents of the documents are relied upon, the interests affected by their disclosure; (b) where the class of documents is invoked, whether the public interest immunity for the class is said to protect; (c) the extent to which the interests referred to have become attenuated by the passage of time or the occurrence of intervening events since the matters contained in the documents themselves came into existence; (d) the seriousness of the issues in relation to which production is sought; (e) the likelihood that production of the documents will affect the outcome of the case; (f) the likelihood of injustice if the documents are not produced."

Journalism has been interpreted as 'the process of gathering, selecting, interpreting, and disseminating news'.[489] While news would ordinarily be the most common type of output of journalism, the definition of news itself may be vague. Further, it has also been argued that news would not be the only output of journalism. For example, opinions may be a relevant output of journalism.[490] Thus the definition of journalism is continuously expanding, and adequate care must be taken to make it inclusive.[491]

This also leads to the question of whether anyone who engages in journalism could be deemed a journalist and accorded the journalistic exemption or if there needs to exist a definition of journalist as well. Who a journalist could be, may be characterised by factors such as the medium of publication, the hierarchy she operates in, the activities she engaged in, the output she delivers, the social role of her work and the ethics followed by her.[492]

Recently citizen journalists have started to occupy a presence in the market for news given the ease of access to internet which allows citizens to publish in real time to a worldwide audience.[493] Therefore, constraining the definition of a journalist to someone employed by a media organisation would exclude a sizeable proportion of people who disseminate news to the public. Thus, factors such as how often a person does activities for a journalistic purpose or whether they obtain their livelihood from carrying out activities for a journalistic purpose may be better suited in determining who a journalist is.

(ii) Ethics Standards

[489] Donald H. Johnston, Journalism and the Media (1979) at p. 2-3 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[490] Kimberly Meltzer, The Hierarchy of Journalistic Cultural Authority: Journalists' Perspectives According to News Medium, 3 Journalism Practice (2009) at pp 59, 62 and 71–72 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[491] Guidance may be taken from other jurisdictions which have aimed to understand what journalistic activities entail. For example, in Australia 'journalism' has been understood as collection, preparation for dissemination or dissemination of material to make available to the public where such material is in the character of news, current affairs or a documentary, or an opinion or analysis of any of these, see Chapter 42: Journalism Exemption in Australian Law Reform Commission, Australian Privacy Law and Practice (ALRC Report 108); In the UK, the journalism exemption is constrained by conditions like the data should have been processed with a view to publish and that such publication should be in public interest and should not be incompatible with journalism, see Section 32, UK DPA.

[492] Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[493] Dan Gillmor, We The Media: Grassroots Journalism By The People, For The People (2006) as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

Finally, to be accorded an exemption from the data protection law, journalists should be bound by ethics standards like honesty and fairness in collecting and disseminating personal data for the purpose of news reporting. The purpose of having ethics standards in place for the application of the journalistic exemption is to be able to 'separate credible contributors from less credible ones by establishing benchmarks of professional practice and measuring people against them'.[494] Ethics standards have become especially important in the age of the internet which has made publishing infinitely easier, with the result that persons without the skills or training in becoming a journalist are becoming the source for news.[495] The lack of any professional qualification examination further intensifies this problem.

To ensure accountability on the part of media houses engaging in journalism, the ALRC was of the opinion that all media houses should be publicly committed to observe published privacy standards which are considered adequate by the data protection regulatory authority.[496] This is a proposal that deserves to be adhered to.

Further, News Broadcasters Association in its submission to the Committee outlined some ethics standards that journalists should adhere to: (i) facts that are published should be accurate, fair, neutral, objective, relevant and impartial; (ii) data should be kept securely; (iii) the publication should be with the aim of dissemination of information, opinions and ideas to the public; and (iv) personal data should be processed while considering the data principals' right to privacy.[497] Such ethics standards may be set by various regulatory organisations in the media, and journalists who adhere to these standards should be accorded the exemption under the data protection law. Independent journalists may self-certify through a declaration that they are adhering to the aforementioned ethics standards.

(b) Scope

As discussed above, to be able to strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term 'journalistic purposes' signifies, and whether an activity for such purposes furthers public interest. From a careful review of public comments and jurisprudential guidance from India and other countries, this would mean that an activity for a journalistic purpose would necessarily have to be linked with an intention to publish or disseminate content, and for such publication or dissemination to occur in public interest.

---

[494] Erik Ugland and Jennifer Henderson, Who Is a Journalist and Why Does It Matter? Disentangling the Legal and Ethical Arguments, 22 Journal of Mass Media Ethics (2007) at p. 243 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[495] Alan Knight, Who is a Journalist? 9 Journalism Studies (2008) at p. 117 as cited in Jonathan Peters and Edson C. Tandoc Jr., People Who Aren't Really Reporters at All, Who Have No Professional Qualifications: Defining a Journalist and Deciding Who May Claim the Privileges, New York University Journal of Legislation and Public Policy (2013).

[496] See Chapter 42: Journalism Exemption, Australian Privacy Law and Practice (ALRC Report 108).

[497] Comments in response to the White Paper submitted by News Broadcasters Association on 31 January 2018, available on file with the Committee.

To infuse a measure of accountability, persons or entities being granted this exemption should be bound to follow ethical standards which sufficiently protect the privacy of data principals which are set out by various regulatory organisations in the media. A public commitment of this nature should be made mandatory.

This would apply to the processing of both personal and sensitive personal data.

(c) Application of Obligations

The standards of specificity as ordinarily required under purpose limitation should not apply in case of journalistic exemption since it is often exploratory in nature and it would be impractical to expect a journalist to specify in exact terms the purposes the personal data is being collected for. Purpose limitation will not apply, though to the extent possible, journalists should still be expected to outline the broad contours of the purpose for which the personal data is being collected, with the final purpose being the publishing of news on the subject. Further, personal data processed for the purpose of journalism should ordinarily be deleted when the purpose of such processing has been realised, that is, when the news has been published.

However, to cover new stories journalists may often need to reach for past records of data and the deletion of personal data collected post publishing may make it very difficult to do so. Therefore, under the journalistic exemption storage limitation should not apply so long as it is clear that the personal data is being stored for only for further journalistic purposes. The notice and consent obligation will not apply, especially in cases of investigative journalism where notifying the individual of the collection of information about them would defeat the purpose of the exercise. However, the journalist undertaking such an activity must have a clear reason (usually public interest) which outweighs the violation of privacy. Such an assessment would usually include the importance of the news, the possibility of verification of information, the level of intrusion into the data principal's privacy and the potential impact upon the data principal and third parties.

While codes such as those issued by the Press Council of India stress the importance of privacy, there is a need for more detailed guidance on specific obligations of the nature discussed above. For instance, while the Norms of Journalistic Conduct laid down by the Press Council of India state that in certain situations, consent of the data principal ought to be taken, the list is not comprehensive and does not lay down the consequences of not following these norms.[498] Similarly, the Code of Ethics and Broadcasting Standards released by the National Broadcasting Authority only states that privacy must be respected unless there is a 'clearly established larger and identifiable public interest' without elaborating on factors which would lead to the identification of such public interest. The Codes also do not lay

[498] Press Council of India, Norms of Journalistic Conduct (2010) available at <http://presscouncil.nic.in/OldWebsite/NORMS-2010.pdf> (last accessed on 2 May 2018).

down obligations relating to how long personal data collected during the course of journalism can be retained for, or how it is to be secured, or data principals' rights in such data.[499] It is expected that such matters will be dealt with in codes of ethics that bind journalists obviating the need for the data protection law to impose such obligations on journalists. Therefore, the codes as they exist now will need to be revised to ensure that they act as a sufficient measure of accountability such that the application of journalistic exemption does not lead to undue violation of the data protection rights of data principals.

Security safeguards should be implemented for all personal data processed by journalists. Therefore, they must take reasonable steps to prevent the data's loss, theft or misuse. Those who avail of the exemption should ensure that their published work is not misleading and distinguishes facts from opinions, apart from adhering with ethics standards.

Requests to implement data principal rights like right to access, confirm and correct can be refused by those taking cover of the journalistic exemption because complying with such requests would often be incompatible with journalism. Such requests may be rejected both before and after publication. A request made before publication could be refused since the provision of such information may lead to attempts to block publication or gathering of further information. An exemption from this obligation may also be necessary to stop persons from harassing journalists by inundating them with requests with a view of blocking or slowing down investigation or publishing of a piece of news. The financial and human resource implications of compliance with such requests may also frustrate journalistic activity, especially for independent journalists.

It should be borne in mind that the exemptions from obligations would only apply so long as the personal data is being processed for journalistic purposes and in a fair and reasonable manner. Thus, the basic obligation of fair and reasonable processing would continue to apply, shaped by this context.

VII. Manual Processing by Small Entities

(a) Context

The obligations placed on data fiduciaries as a part of data protection law are largely aimed at ensuring that data principals are not subjected to privacy harms and the obligations placed on fiduciaries are thus designed to mitigate and prevent the harms caused by risky practices arising out of electronic data processing using automated means. Such technologies substantially increase the risk of harm from personal data processing due to the added ease of recording, dissemination, viewing and systematic analysis.[500] An important question that arises is whether all the obligations imposed on entities carrying out such processing need to be imposed on other entities processing by means other than automated ones. While there is a

[499] News Broadcasters Association, New Delhi, Code of Ethics & Broadcasting Standards (2008) available at <http://www.nbanewdelhi.com/assets/uploads/pdf/code_of_ethics_english.pdf> (last accessed on 3 May 2018).
[500] Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stanford Law Review (1998) at p.1198.

risk that such fiduciaries may create privacy harms, the Committee is of the view that they may not need to be subjected to the same legal duties.

(b) Scope

While it may be necessary to ensure that entities carrying out manual processing are subjected to data protection law, it is also important to ensure that any exemption from burdensome obligations that has been designed specifically for them does not become a loophole through which organisations execute their most harmful activities. For instance, the small business exemption in Australia[501] is criticized as being too broad, allowing for large swathes of processing activities to go unchecked.[502] Any such exemption should thus only be held out to those entities that would relatively have to bear the heaviest burdens from data protection obligations despite carrying out activities that only raise limited privacy risks. A turnover-based exemption appears to cover those entities that would suffer the most from legal obligations and such a scheme may be seen in some legal regimes.[503] However, this may not make for an appropriate classification as many entities with little or no turnover may nonetheless be processing large volumes of personal data and may, therefore, give rise to substantial harm. The Committee is thus of the view that apart from a turnover-based condition, to avail of this exemption an entity should not process personal data of data principals exceeding a specified number calculated over a definite time period. It must also not collect personal data for the purpose of disclosing it to other parties. In this manner, the exemption may be restricted to small entities processing a limited amount of personal data manually without any intention of further disclosure.

(c) Application of Obligations

The obligations from which the entity is to be exempted must similarly be restricted to the most burdensome or costly ones, without limiting the essential protections that data protection law otherwise offers. Obligations that may be onerous in this context are notice, data quality, storage limitation, certain aspects of the right to access, the right to portability, and the right to be forgotten (which is largely inapplicable in this case), apart from organizational measures related to privacy by design, transparency and security safeguards. These leave in place core obligations regarding purpose and collection limitation as well as data principal rights such as confirmation, access and correction.

---

[501] See Section 6D of the Privacy Act, 1988 (pegging the threshold for the annual turnover of a 'small business operator' at $3 million, apart from placing other conditions).

[502] See, comments in response to the White Paper submitted by Graham Greenleaf on 31 January 2018, available on file with the Committee, at p. 8 (remarking that Australia may be the only country with such a small business exemption with its application extending to 94% of all businesses).

[503] Such exemptions exist in India, for example, for the merger control regime under the Competition Act, 2002 (see, Ministry of Corporate Affairs, Government of India, Notification regarding Target Exemption available at <http://www.cci.gov.in/sites/default/files/notification/SO%20673%28E%29-674%28E%29-675%28E%29.pdf> (last accessed on 26 May 2018)), and for licensing requirements under the Food Safety and Standards Act, 2006 (see, Regulation 1.2.1(4), Food Safety and Standards (Licensing and Registration of Food Business) Regulations, 2011).

RECOMMENDATIONS

Non-Consensual Grounds of Processing

- Functions of the State: Welfare functions of the state will be recognised as a separate ground for processing. Processing activities carried out by the State under law will be covered under this ground, ensuring that it is in furtherance of public interest and governance. However, only bodies covered under Article 12 of the Constitution may rely on this ground. Processing towards activities that may not be considered part of a welfare functions would, however, not to be permitted. Thus, the availability of this ground is restricted to certain entities and certain functions to avoid vagueness in the law. **[Sections 13 and 19 of the Bill]**

- Compliance with Law or Order of Court or Tribunal: Compliance with law or order of court or tribunal will be recognised as a separate ground for processing to avoid inconsistency with obligations under other laws, regulations and judicial orders. The word 'law' shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications that have statutory authority. Order of court or tribunal would be restricted to Indian courts and tribunals. Obligations imposed by contract, foreign law and foreign judicial orders shall not be permitted to be processed under this ground. **[Sections 14 and 20 of the Bill]**

- Prompt Action: Prompt action will be recognised as a separate ground for processing. It should receive a strict interpretation and only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary to meet emergency situations. **[Sections 15 and 21 of the Bill]**

- Employment: Employment will be recognised as a separate ground for processing. This ground should be invoked only where processing under consent would involve disproportionate effort or where the employment relation makes consent inappropriate and will permit processing even where employment-related activities are not authorised under any of the other grounds of processing such as compliance with law. **[Section 16 of the Bill]**

- Reasonable Purpose: Reasonable purpose is a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The ambit of the provision would be limited to those purposes which are whitelisted by the DPA to guide data fiduciaries. **[Section 17 of the Bill]**

Exemptions

- Security of the State: The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is necessary in the interest of the security of the state. Any restriction must be proportionate and narrowly tailored to the stated purpose. The Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities. **[Section 42 of the Bill]**

- Prevention, Detection, Investigation and Prosecution of Contraventions of Law: The data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law (including protection of revenue). In order to invoke the exemption, the law enforcement agencies must be authorised by law. **[Section 43 of the Bill]**

- Disclosure for the Purpose of Legal Proceedings: The disclosure of personal data necessary for enforcing a legal right or claim, for seeking any relief, defending any charge, opposing any claim or for obtaining legal advice from an advocate in an impending legal proceeding would be exempt from the application of the data protection law. General obligations of security and fair and reasonable processing will continue to apply. **[Section 44 of the Bill]**

- Research Activities: The research exemption is not envisaged as a blanket exemption. Only those obligations that are necessary to achieve the object of the research will be exempted by the DPA. This assessment is contextual and dependent on the nature of the research. **[Section 45 of the Bill]**

- Personal or Domestic Purposes: A narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. It would provide a blanket exemption from the application of the data protection law. **[Section 46 of the Bill]**

- Journalistic Activities: To strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term 'journalistic purposes' signifies, and how ethical standards for such activities would need to be set. Where these conditions are met, an exemption should be provided. **[Section 47 of the Bill]**

- Manual Processing by Small Entities: Since the risk of privacy harms being caused are higher when personal data is processed through automated means, an exemption will be made in the data protection law for manual processing by data fiduciaries that are unlikely to cause significant harm and would suffer the heaviest relative burdens from certain obligations under this law. **[Section 48 of the Bill]**

CHAPTER 9: ENFORCEMENT

Ultimately, any law is only as good as its enforcement. To ensure that India enjoys a robust data protection regime which ensures that its substantive obligations are respected, a competent enforcement mechanism is of the utmost importance. This chapter sets out the means by which accountability for obligations on entities is ensured in a fair and effective manner.

Based on a review of the theoretical literature, practical experience of other countries in enforcing data protection laws, the experience of our own country with respect to enforcement and public comments to our White Paper, a responsive regulatory framework equipped with a range of tools has been found by us to be of critical importance.[504] Enforcement should, where possible, be front-ended, i.e. require *ex ante* compliance by entities with substantive obligations under the law. Where determination of liability for violations is required, a well-resourced DPA, with necessary powers is required to be set up. Given the scale of enforcement, such DPA must work closely with sectoral regulators and self-regulatory or industry bodies, both to formulate codes of practice relating to several issues of data protection as well as to prevent any regulatory overlap in determining liability.

This chapter sets out the aforementioned framework in three sections: first, the structure and functions of the regulator (the DPA) and the tools that will be used for regulation; second, the classification of and obligations on certain data fiduciaries that will be regulated; and third, the remedies available in case of violations of the provisions set out under the data protection law.

In making recommendations on the issues arising in relation to enforcement of a data protection law, the Committee has relied on several helpful public submissions made to the White Paper, particularly those by Dvara Research[505] and NIPFP *et al.*[506]

A. The Data Protection Authority: Structure, Functions and Tools

I. White Paper and Public Comments

After conducting a preliminary study of other jurisdictions, the White Paper suggested the creation of an independent regulatory body for enforcement of a data protection legal framework. Further, it was suggested that this regulatory body should have the powers of (a) monitoring, enforcement and investigation; (b) awareness generation; and (c) standard setting. It was suggested that a number of regulatory tools and mechanisms such as codes of

[504] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspective (Oxford University Press, 2014).
[505] Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.
[506] Comments in response to the White Paper submitted by the National Institute of Public Finance and Policy, Mozilla Foundation and Vrinda Bhandari, available on file with the Committee.

practice and categorisation of data fiduciaries could be deployed to achieve enforcement objectives.[507]

Most commenters were of the view that a separate, independent authority needs to be constituted to carry out general functions related to data protection. Favoured measures for maintaining the independence of the body include fixed tenure, disclosure of conflicts, post-retirement safeguards and restrictions on future employment, and financial independence. Various commenters suggested that the functions of the DPA should involve investigation, registration, standard-setting and adequacy assessments. The recommended composition includes a chairperson and members with technical and legal expertise. They should be appointed by a committee composed of members from the judiciary, the executive, civil society, and industry representatives. In addition, some commenters opined that state level authorities may be necessary in sharing the considerable regulatory burden; while others argued that allowing state authorities would result in an increase in costs, threat of double prosecution, and inconsistency in the applicable legal position.

Most commenters were of the view that an individual whose data protection rights have been violated may first approach the grievance redressal officer of the data fiduciary. Where the data fiduciary fails to resolve the complaint of the individual in a satisfactory or expeditious manner, the data principal may approach the DPA for recourse. The DPA may also initiate action against a data fiduciary on a *suo motu* basis. Qualifications of the adjudicating officer, as suggested by the commenters, include a graduate degree or its equivalent, and specific expertise in law and information technology. The commenters were in agreement that the adjudicating officer should have the powers of a civil court and be able grant compensation as well as impose monetary penalties. Most commenters were of the view that an appeal from the order of the adjudicating officer may lie with a specialised data protection appellate tribunal. These views have been fully considered while laying out the enforcement structure below.

II. Analysis

(a) Structure and Functions of the DPA

(i) Establishment

The DPA shall be in the nature of a high-powered, independent national body in view of the significance of creating an ecosystem of responsible data handling. The DPA, a sector-agnostic body, will ensure that every entity that handles data is conscious of its obligations and that it will be held to account in case of failure to comply. The DPA shall be a body corporate having perpetual succession and a common seal with the power to acquire, hold or dispose of property. Further, it will have the capacity to contract and to sue or be sued. It

[507] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 2.

shall be a single institution with appropriate regional offices in order to fulfil its various statutory functions.[508]

(ii) Composition

It is important to create a system for selecting members of the DPA in a fair and transparent manner, especially because it is expected that government agencies will be regulated as data fiduciaries under the data protection law. The DPA will be governed by a board consisting of six whole-time members and a chairperson appointed by the Central Government on the recommendation of a selection committee. The selection committee shall consist of the Chief Justice of India or her nominee (who is a judge of the Supreme Court of India), the Cabinet Secretary, Government of India, and one expert of repute who has special knowledge of, and professional experience in areas related to data protection, information technology, data management, data science, cyber and internet laws and related subjects.[509]

The members of the DPA should be individuals of integrity and ability with special knowledge of, and professional experience of not less than 10 years in, areas related to data protection, information technology, data management, data science, cyber and internet laws and related subjects.[510] Following this mechanism for selection and appointment is aimed at ensuring independence, expertise and non-partisanship in selecting members of the DPA.[511]

To ensure the independence of the members of the DPA, their employment shall be fixed for a term of five years subject to a suitable retirement age.[512] The salaries and allowances should be prescribed by the Central Government. However, the terms and conditions of appointment of such members should not be changed to their disadvantage during their tenure. Furthermore, the members of the DPA shall not be permitted to accept employment either under the Central or State Governments, or under a significant data fiduciary, during the course of their tenure or for a period of two years thereafter.

(iii) Functions of the DPA

Broadly, the DPA may have four departments that shall perform the following functions: (1) monitoring and enforcement; (2) legal affairs, policy and standard setting; (3) research and

[508] Section 3, SEBI Act. The SEBI Act has a similar provision establishing SEBI.
[509] See similar provisions in Section 9, Competition Act; Sections 4(4), SEBI Act; Section 4, TRAI Act; Section 3, IRDA Act.
[510] See similar provisions in Section 8, Competition Act; Section 4(5), SEBI Act; Section 4, TRAI Act; Section 4, IRDA Act. . Inputs regarding qualifications of members of the DPA are adopted from Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.
[511] Report of the Financial Sector Legislative Reforms Commission, Volume 1: Analysis and Recommendations (2013).
[512] See similar positions in Section 10, Competition Act; Section 5, SEBI Act; Section 5, IRDA Act; and Section 5, TRAI Act.

awareness; and (4) inquiries, grievance handling and adjudication.[513] We have set out key particulars of each broad category below:

Monitoring and Enforcement

(i) Monitoring and ensuring compliance, with the provisions of the data protection law;
(ii) Issuance, renewal and revocation of registration certificates to data auditors and issuing a code of conduct for such auditors;
(iii) Registration of significant data fiduciaries;
(iv) Processing data breach notifications and taking action accordingly;
(v) Assessing data audits;
(vi) Monitoring cross-border transfer of personal data;
(vii) Specifying circumstances where a DPIA may be required;
(viii) Maintaining a database containing names of significant data fiduciaries and their rating in the form of data trust scores indicating compliance with obligations under the data protection law; and
(ix) Specifying any other fee or charges, where relevant.

Legal Affairs, Policy and Standard Setting

(i) Whitelisting activities processed under the ground of reasonable purpose;
(ii) Making recommendations to the Central Government for green-lighting countries for cross-border transfer of personal data;
(iii) Specifying residuary categories of sensitive personal data;
(iv) Issuance of codes of practice;
(v) Advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data in accordance with the provisions of the data protection law;
(vi) Advising the Central Government on acceding to any international instrument relating to data protection; and
(vii) Issuing any guidance documents that may be necessary for the interpretation or suitable implementation of this law.

Research and Awareness

(i) Generating awareness amongst data principals on their rights and the means to exercise them;[514]

[513] The structure and functions of the DPA have been adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee.
[514] Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at < https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.16.

(ii) Promoting public awareness in understanding the risks, rules, safeguards and rights with respect to data protection including issuance of any public statement setting out trends in or specific instances of contravention of the provisions of the law;
(iii) Educating data fiduciaries regarding data protection best practices and their obligations under the law;
(iv) Monitoring technological developments and commercial practices which may affect data protection practices;[515] and
(v) Promoting measures and undertaking research for innovation in the field of data protection.[516]

The Committee finds it appropriate to point out that data protection law, even after the enactment of a general statute as proposed in this report, would still be in a nascent stage in India. The institutional structures and bodies of knowledge supporting the privacy of Indians would not develop unsupported in the course of the implementation of the law. It is thus imperative that a dedicated research wing be put into place within the structure of the DPA and that such wing work closely with the policy-making departments of the DPA to ensure the quality and effectiveness of its work.[517] This may extend into research regarding technical aspects of data protection, forensic data analysis practices, detection of uncharacteristic and unusual processing, algorithmic impact assessments, international practices as well as transnational flows of data, and other unique aspects of informational policy.

Inquiries, Grievance Handling and Adjudication

(i) Calling for information, and undertaking inspections or inquiries into the affairs of data fiduciaries in accordance with the law;
(ii) Delivering efficient, well informed, proportionate and timely enforcement actions;[518] and
(iii) Interfacing with the data principal for handling complaints.[519]
(iv) Separate adjudication wing for adjudicating disputes (discussed below).

[515] For example, in the current technological scenario, the DPA should focus on the development of Internet of Things, AI and Big Data.
[516] For example, this research can take the form of a peer reviewed journal, thought leadership in the form of original articles and reports, establishment of doctoral chairs etc.
[517] Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.16.
[518] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee. Such measures may include issuing a warning or a reprimand, requiring the data fiduciary to cease from taking a specific action, etc.
[519] This wing shall create an efficient infrastructure to receive and monitor the complaints of data principals. Complaints should be accepted via email, online portal, telephone, letter or in-person. Further, with changing technology, additional means of lodging complaints should be adopted.

(b) Enforcement Tools

Under the model of responsive regulation, it has been suggested that the ideal method of enforcing compliance with the law is to adopt an "enforcement pyramid".[520] Through this approach, regulators match the seriousness of the contravention with the severity of the sanction and resort to coercive sanctions only when the less interventionist methods would fail to ensure compliance. These measures should include both sanctions following contraventions as well as *ex-ante* tools which would allow the DPA to enforce the law.

An indicative list of the tools that should be made available to the DPA in the enforcement pyramid is below[521]:

(i) Issuance of a Direction

The DPA should be given the power to issue directions from time to time as it may consider necessary to data fiduciaries and data processors either generally or to particular data fiduciaries and processors for discharging its functions under the law. Such fiduciaries and processors shall be bound to comply with these directions.[522]

(ii) Power to call for Information

The DPA will have the power to require a data fiduciary or data processor to provide such information, as may be necessary for performing its functions under the law. When calling for information, the DPA ought to specify the format and time in which such information is to be provided.[523]

---

[520] See Chapter 50: Enforcing the Privacy Act, Australian Privacy Law and Practice (ALRC Report 108). The ALRC Report refers to J Braithwaite, To Punish or Persuade: Enforcement of Coal Mine Safety (1985); B Fisse and J Braithwaite, Corporations, Crime and Accountability (1993); C Dellit and B Fisse, Civil and Criminal Liability Under Australian Securities Regulation, The Possibility of Strategic Enforcement in G Walker and B Fisse (eds), Securities Regulation in Australia and New Zealand (1994) at p. 570; Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p. 9.

[521] Indicative tools set out below are adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; EU GDPR and commonly available enforcement tools seen under Indian statutes like SEBI Act, Insurance Act and so on. See also Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at pp 10-12.

[522] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.11

[523] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.10.

(iii) Publication of Guidance

The DPA should inculcate a culture of openness where it encourages queries being posed to it by various stakeholders to clarify positions in the law. It could also issue guidance where it is of the view that a particular provision under the data protection law requires additional clarification. These responses could then be published on the DPA website to serve as guidance for the general public.[524]

(iv) Issuance of a Public Statement

The DPA may also issue public statements through its website regarding either trends of contraventions of the law by certain groups of data fiduciaries or of specific instances of contraventions to both heighten public awareness on the issue as well as to serve as a deterrent against infringements of the law.[525]

(v) Codes of Practice

The development of a good code of practice is fundamental to the functioning of a balanced data protection framework. A code of practice supplements the law, filling gaps with details that cannot be provided in legislation, thereby helping in better implementation of the principles the law is founded upon. The DPA will have the authority to issue codes of practices on its own, or it may approve codes of practice submitted by industry or trade associations representing the interests of data principals, sectoral regulators or statutory authorities. Before issuing or approving a code of practice, the DPA will be under an obligation to undertake a consultation process with appropriate sectoral regulators and other stakeholders, including data fiduciaries to take into account the developments taking place in the relevant industry. This is to ensure that codes of practice are issued in a transparent and democratic manner. Such codes of practice as issued by the DPA shall always be subject to the provisions of the applicable law.

The non-compliance with such codes of practice may be considered by the DPA, or any court or tribunal, in determining whether a data fiduciary or data processor (as the case may be and to the extent applicable) has violated provisions of the law. The concerned data fiduciary or data processor may however prove that it has adopted an equivalent or higher standard than the one stipulated in the relevant code of practice.

[524] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.10.

[525] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.11

(vi) Conducting Inquiries

The DPA may conduct an inquiry where it has a reasonable ground to believe that certain activities of the data fiduciary are likely to detrimentally affect the interests of a data principal; or that a data fiduciary has violated any of the provisions of the data protection law. To achieve this aim, the DPA should have the power to appoint inquiry officers to inquire into the affairs of the data fiduciary. The inquiry officer shall call for the requisite documents, books, records, etc. of the data fiduciary and examine any officer or employee of the data fiduciary for the purposes of inquiry. Moreover, the DPA should also have the power to conduct searches and seize documents and other material as may be required for the purposes of enforcement.

(vii) Injunctive Relief

Pursuant to its power of conducting an inquiry, the DPA shall have the powers to issue warnings, reprimands, order data fiduciaries to cease and desist from causing violations of the law, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law, suspend or discontinue any cross-border flow of personal data, cancel or suspend any registration granted by the DPA and take any other action as it may see fit to ensure compliance with the law.

(viii) Inter-sectoral coordination

It is relevant to mention that since the DPA will be dealing with a subject matter on which other regulators or authorities set up under a law made by the Parliament or any state legislature may also exercise concurrent jurisdiction, the DPA shall consult such regulators and authorities before taking any action under the proposed data protection legal framework and also enter into a memorandum of understanding with such regulators and authorities governing the coordination of such action.[526]

(c) Adjudication Wing of the DPA

In addition, the DPA shall also have a separate and independent Adjudication Wing which shall consist of such number of Adjudicating Officers as the Central Government may prescribe. The Central Government must undertake a capacity assessment exercise before determining the number of Adjudicating Officers who would be part of this office. Such officers should be individuals of integrity and ability and must have special knowledge of, and professional experience of not less than 7 years in areas related to constitutional law,

[526] Adopted from the comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al,* Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at pp 12, 14.

information technology law and policy, cyber and internet laws and related subjects.[527] Further, the terms and conditions of appointment of such Adjudicating Officers must ensure their independence. The Adjudication Wing should function at arm's length from the remaining wings of the DPA which deal with legislative matters and executive enforcement. The Adjudicating Officers shall have the power to conduct an enquiry and adjudicate any dispute arising between data fiduciaries and data principals, including availing any compensation. Further, the Adjudicating Officer may also impose monetary penalties where the data fiduciary has contravened the provisions of the law.[528]

(d) Appellate Tribunal

An appellate tribunal shall be set up to hear and dispose of any appeals from the orders of the DPA and the orders of the Adjudicating Officers under the Adjudication Wing of the DPA. Such a tribunal should consist of a chairperson and such number of members as notified by the Central Government. The Central Government may also confer powers on an existing tribunal for this purpose if it believes that any existing tribunal is competent to discharge the functions of the appellate tribunal envisaged under the data protection law. The orders of the appellate tribunal will be finally appealable to the Supreme Court of India.

B. The Regulated Entities: Classification and Obligations

I. White Paper and Public Comments

The provisional view of the White Paper suggested the creation of differentiated obligations for certain entities whose processing activities create higher degrees of risk or may cause significant harm for better enforcement.[529]

Most commenters were in favour of some form of categorisation of entities to be regulated under the law. It was commonly suggested that fiduciaries processing sensitive personal data should be dealt with separately. Other criteria for categorisation included public or private nature of the entity, breadth of aggregation of data, inherent risks in the nature of the processing activity, scale of operations, turnover, sector of operations, range of products, and services offered. If a special category of data fiduciaries were to be created, a majority of the

[527] Section 8, Competition Act; Section 15I, SEBI Act.

[528] Inputs taken from the SEBI Act; Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee; Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018) at p.16.

[529] White Paper of the Committee of Experts on a Data Protection Framework for India available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 2C.
In this context, the Committee also notes the Comments in response to the White Paper submitted by Dvara Research on 2 April 2018, available on file with the Committee as well as Beni Chugh *et al*, Dvara Research Working Paper Series No. WP-2018-01 (July 2018) available at <https://www.dvara.com/blog/wp-content/uploads/2018/07/Effective-Enforcement-of-a-Data-Protection-Regime.pdf> (last accessed on 24 July 2018).

commenters agreed that they should have additional obligations, such as mandatory registration, DPIAs, data audits, and a DPO. A few commenters suggested alternative obligations on entities such as maintaining records of processing activities, frequent supervision, higher reporting obligations, review or audit of data security and data breach mitigation plans.

The perspective on registration of data fiduciaries was split. Those who favoured it thought that it would assist in monitoring and identification of entities. Those who opposed it argued that it would add substantial compliance cost and an entry barrier, which would in turn discourage ease of doing business in India. Regarding audits, commenters were conflicted on whether they should be conducted internally or by empanelled external firms. Those who favoured some form of external audits argued that it ensured transparency, credibility, removal of bias, and accuracy. Most commenters favoured the requirement for a DPO in regulated entities. Some attempted to temper the requirement by arguing that the DPO need not be located in India. The functions that commenters sought to allocate to the DPO include advising, compliance monitoring, ensuring accountability, performing audits and DPIAs, cooperating with the regulator, training staff, grievance redressal, acting as the contact person on data protection matters, and monitoring security safeguards.

II. Analysis

(a) Significant Data Fiduciaries

The Committee is of the opinion that it is important to distinguish and place additional obligations on entities which are capable of causing significantly greater harm to data principals as a consequence of their data processing activities. This categorisation of data fiduciaries will enable the DPA to treat data fiduciaries who have the potential to cause greater harm on a separate track.

The categorisation will be based on an overall assessment of the following parameters: volume of the personal data being processed, nature of data (sensitive or not), volume of personal data processed, type of processing activity undertaken (collection, use, disclosure), turnover of the data fiduciary, the risk of harm resulting from any processing undertaken, whether the data fiduciary is making use of any new kind of technology to carry out the processing activity, or the presence of any other harm which is likely to cause harm to the data fiduciary. These broad parameters will be set out in the law and the DPA will have the power to lay down specific details/thresholds to identify such entities, who will be classified as significant data fiduciaries.

Significant data fiduciaries ought to have, at a minimum, the following additional obligations - (i) Registration with the DPA; (ii) DPIA; (iii) Record-keeping; (iv) Data audits; and (v) Appointment of DPO. However, where the DPA is of the view that processing undertaken by a data fiduciary (not being a significant data fiduciary) carries a risk of significant harm to data principals, it may notify the application of these obligations on such data fiduciaries.

(i) Registration

The DPA will have to oversee a large regulatory space criss-crossing different organisations in a variety of sectors. Consequently, it will be onerous for the DPA to identify each such data fiduciary that may cause significant harm. In order to solve this problem, significant data fiduciaries will have to register with the DPA. The process of registration is intended to be a notification by an entity which fulfils the threshold criteria of a significant data fiduciary, it is not akin to a licensing requirement to carry on business.

(ii) Data Protection Impact Assessment

The use of new technologies, large-scale profiling, and use of sensitive personal data like biometric and genetic information are activities with potential to endanger data principals' interests in the event of a security breach.[530] Before commencing any of the aforementioned activities, significant data fiduciaries would be required to conduct an assessment of the impact such a project is likely to have on the data principals affected by such change and set out the means of reducing or eliminating such impact through a DPIA. The DPA would publish a list of situations when such an assessment would need to be conducted. Though the impact assessment is envisaged as an internal organisational measure, there may also be situations where an external data auditor (as discussed below) should be engaged by the fiduciary to carry out a DPIA. The DPA must determine what these situations are.
The DPIA should contain the following:

1. description of the nature, scope, context and purpose of processing;
2. necessity and proportionality of processing;
3. risks posed to the data principals' personal data and harms likely to be caused to a data principal; and
4. measures that could be deployed to reduce or eliminate these risks.

The DPIA must be submitted to the DPA who may then choose to advise the significant data fiduciary on the areas which may need further analysis or action on the part of the data fiduciary. It may direct the fiduciary to cease the processing or carry it out subject to conditions it imposes.

(iii) Record-keeping

Under the principle of accountability, data fiduciaries are required to be able to demonstrate that any processing undertaken by them are in accordance with data protection law. As a part of this obligation, it would often be necessary that verifiable and authentic records are

[530] UK Information Commissioner's Office's Guide to the GDPR, Data protection impact assessments available at <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>, (last accessed on 26 April 2018).

maintained by them regarding the processing operations that they undertake. Nonetheless, for abundant caution, the Committee finds it appropriate that a separate obligation be in place requiring significant data fiduciaries to maintain accurate and up-to-date records regarding particularly important processing operations as well as the results of any security safeguard review, reports from data protection impact assessments and other aspects that may be specified by the DPA. This obligation would ensure that these fiduciaries are able to cooperate with the DPA and would permit monitoring of the relevant operations.[531] Given the volume, pervasiveness and risks of leakage of data related to processing by State entities, the Committee also finds it appropriate to mandatorily require such entities to maintain records.

(iv) Data Audits

Data audits should be undertaken by independent external auditors empanelled by the DPA to assess whether a significant data fiduciary's processing activities and policies are in compliance with the applicable data protection law. As highlighted by commenters, having external auditors will ensure transparency and credibility.[532] Besides, it will not be feasible for the DPA itself to conduct audits for all significant data fiduciaries. It is our view that a new profession of data auditors will have to be created to comply with norms in this law and other sector-specific regulation pertaining to data handling. The qualification of auditors should be determined by delegated legislation.[533] Though this obligation is envisaged as recurring on a regular basis (for instance, annually) it is appropriate to empower the DPA to require data fiduciaries to conduct audits on other occasions in situations where it is likely that harm would be caused to data principals. In such situations, it is necessary for the DPA to appoint an auditor for this purpose.

A data audit shall include an analysis of compliance with obligations set out under the data protection law such as purpose and collection limitation, storage limitation, organisational and security measures undertaken, responses to grievance and requests, DPIAs undertaken, clarity of privacy policies and consent forms, and processing activities of children. On the basis of the audit, a rating in the form of a data trust score (indicating compliance with the obligations under the data protection law) may be assigned to such significant data fiduciaries by the data auditor having regard to any criteria that may be specified by the DPA in this regard.

---

[531] Recital 82, EU GDPR.

[532] UK Information Commissioner's Office, Auditing Data Protection - A Guide to ICO Data Protection Audits available at <https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf> (last accessed on 30 April 2018); Adopted from comments in response to the White Paper submitted by Pramod Rao Citibank on 31 January 2018, available on file with the Committee.

[533] By way of comparison, in the UK, the qualifications for an auditor are that they should be IIA (Institute of Internal Auditors) qualified and hold the ISEB (Information Systems Examination Board) Certificate in Data Protection (or be working towards those qualifications). Further, a range of skills and backgrounds including data protection casework, the banking sector, IT services and financial audit; UK Information Commissioner's Office, Auditing Data Protection - A Guide to ICO Data Protection Audits available at <https://ico.org.uk/media/for-organisations/documents/2787/guide-to-data-protection-audits.pdf> (last accessed on 30 April 2018). In Australia, under Section 26A(3), Privacy Act, 1988, the Privacy Commissioner for audit purposes, "may engage as consultants persons with suitable qualifications and experience. The terms and conditions on which a consultant is engaged are as determined by the Commissioner."

(v) Data Protection Officer

Given that significant data fiduciaries may process considerably sensitive and large amounts of personal data, it is essential that they appoint a person who facilitates compliance with data protection laws by monitoring and advising these fiduciaries as well as acts as a point of contact with the DPA. The eligibility and qualification requirements of the DPO will be specified by way of delegated legislation. The functions allocated to such DPO could include compliance monitoring, developing and ensuring robust compliance and accountability procedures, cooperating with the DPA, training staff, conducting DPIAs, grievance redressal, monitoring security safeguards, and maintaining records, etc.

C. Penalties, Compensation and Offences

I. White Paper and Public Comments

The White Paper considered several models of imposition of a monetary penalty on data fiduciaries found to be in violation of the data protection law, which included a per-day penalty, a penalty based on the discretion of the adjudicatory body which would be subject to a fixed upper limit and finally one where the discretion is subject to an upper limit which is a variable parameter. The White Paper provisionally concluded that the highest form of deterrence in relation to civil penalties may be where a per day civil penalty is imposed subject to a fixed upper limit or a percentage of the total worldwide turnover of the defaulting data controller of the previous financial year, whichever is higher. Further, the White Paper concluded that an individual may be given a right to seek compensation when she has suffered a loss or damage as a result of an infringement of the data protection law.[534]

Some commenters suggested that penalties should either have a fixed upper limit, or be based on a percentage of the turnover of the entity. According to the commenters, some contraventions by fiduciaries which ought to warrant penalties include: unlawful processing of personal data, unauthorised disclosure of personal data, failure to implement security measures, and violation of individual rights.

Commenters were also of the view that data principals who suffer "material or non-material damage" may be considered where "non-material damage or harm" should include breach of privacy, mental distress, reputational harm, discrimination, etc.

Further, in the case of an offence, commenters suggested that fines along with imprisonment should be imposed on data fiduciaries in certain, specific instances of violations of the data protection law where *mala fide* intent or recklessness is involved. A few commenters also suggested that only wilful non-compliance with the orders of the DPA should be punished with criminal liability.

[534] White Paper of the Committee of Experts on a Data Protection Framework for India, available at <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf> (last accessed on 20 April 2018) at Part IV, Chapter 4.

II. Analysis

(a) Burden of Proof and Accountability

When seeking a remedy under the law, it would have to be demonstrated that the data fiduciary has violated any provisions of the law or any harm has been suffered by the data principal as a result of such violation. Once this has been established, to mitigate any liability, the data fiduciary would have to prove, *inter alia*, that it has complied with the provisions of the law and undertaken all necessary and requisite measures to prevent any harm. It is necessary to note, however, that in relation with the conditions for the validity of consent, the burden of proof should specifically be placed on the data fiduciary.

(b) Penalties

The Adjudicating Officer under the Adjudication Wing of the DPA should have the power of imposing monetary penalties on infringing data fiduciaries. Civil penalties have been acknowledged as an effective method of ensuring deterrence.[535] Penalty imposed should be such which will make it unprofitable for data fiduciaries to be engaging in the wrongful act in the future and will be proportional to the harm suffered by the data principal. Obviously, the amount cannot be set at either extreme of excessive penalisation which would decrease business activity in the sector or minimal penalisation which would not have deterrent value. The Committee is of the view that a penalty of up to a certain percentage of the total worldwide turnover in the preceding financial year of the data fiduciary or a fixed amount set by the law, whichever is higher (and as applicable depending on the type of data fiduciary involved) should be imposed for major infractions of law. The Committee is cognisant of the fact that in today's day and age, data fiduciaries, especially companies incorporated in India, forming part of a group may be processing personal data for their parent, subsidiary or other companies within the same group. In such cases, the Committee is of the view that such group companies may also be penalised where they may have benefitted from any unlawful processing undertaken by the said data fiduciaries. Consequently, the proposed legal framework will set out the formulation to reflect this understanding.[536] Furthermore, the law will also set out penalties based on different formulations for violations involving failure to comply with any request pursuant to data principal rights, failure to furnish reports, information, etc. as mandated under the law.

The final determination of the amount within the range provided should be dependent on factors which would include the following:

---

[535] Max Minzner, Why Agencies Punish, 53(3) William and Mary Law Review (2012); Michelle Welsh, Civil Penalties and Responsive Regulation: The Gap Between Theory And Practice, 33(3) Melbourne University Law Review (2009).

[536] A similar approach is seen in the EU GDPR. Moreover, even in the Indian context, Section 27(b), Competition Act imposes a penalty of "not more than ten percent of the average of the turnover for the last three preceding financial years" for abuse of dominant position. Further, Section 43A, Competition Act penalises up to one percent of the total turnover or the assets, of a combination which has not furnished information to the CCI.

(i) the nature, gravity and duration of the infringement which would depend on the nature, scope or purpose of the processing and the number and sensitivity of data principals affected;
(ii) whether the infringement was intentional or grossly negligent;
(iii) efforts made by the data fiduciary to mitigate the damage caused to the data principals;
(iv) the technical and organisational measures implemented by the data fiduciary including adherence to the code of practice; and
(v) any relevant previous infringement by the data fiduciary.

(c) Compensation

There needs to be certainty in the ascription of liability so that the data principals are not made to run from pillar to post in search of finding the relevant fiduciary or processor in the link who was responsible for the damage caused. Therefore, joint and several liability to pay compensation would be attached to the data fiduciary and its processors with penalty being imposed so long as an infringement has been proven. Therefore, at the first instance, the aggrieved data principal will receive the compensation amount due to her. Thereafter, the division of liabilities of paying compensation will become a second order question.

A remedy needs to be provided under the law to compensate data principals for the harm caused to them due to infringements under the data protection law. The factors for deciding on the quantum of compensation being awarded could be largely similar to the factors set out under the penalties section. These may include the following:

(i) Nature, duration and extent of non-compliance or violation of legal obligation by data fiduciary;
(ii) Nature and extent of harm suffered by the data principal due to the default;
(iii) The intentional or negligent character of the violation;
(iv) Whether the data fiduciary is sufficiently transparent in its data processing activities;
(v) Whether the data fiduciary, or the data processor as the case may be took any measures to mitigate the damage suffered by the data principal;
(vi) Amount of gain or unfair advantage to the data fiduciary, whether quantifiable, due to the default;
(vii) Repetitive nature of the default- whether first time or a subsequent breach and whether there has been any previous instance of such breach;
(viii) Failure to operate policies, procedures and practices to protect personal data;
(ix) Nature of the personal data involved.

(d) Offences

Offences created under the data protection law should be linked to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. Some acts which may be treated as an offence would be: (i) obtaining, transfer, disclosure and sale of personal and sensitive personal data in violation of the provisions of the data protection law such that it caused harm to the data principal; (ii) re-identification and processing of previously de-identified personal data. Such offences may be made cognizable and non-bailable and may be tried by the relevant jurisdictional court. In cases of offences committed by companies, the person in-charge of the conduct of the business of the company, and in the cases of offences by a government department, the head of the department should be held responsible. However, liability should not be imposed on such persons if they can prove that such offence was committed without her consent or that they put in all reasonable efforts to prevent such commission of an offence.

RECOMMENDATIONS

- The data protection law will set up a DPA which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. Broadly, the DPA shall perform the following primary functions: (i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (iv) inquiry, grievance handling and adjudication. **[Chapter X of the Bill]**

- The DPA is vested with the power to categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to data principals as a consequence of their data processing activities. This categorisation will be based on an assessment of volume of the personal data being processed, nature of personal data, type of processing activity undertaken, turnover of the data fiduciary, the risk of harm, and the type of technology used to undertake processing. **[Section 38 of the Bill]**

- Significant data fiduciaries will have to undertake obligations such as: (i) Registration with the DPA; (ii) Data Protection Impact Assessments; (iii) Record-keeping; (iii) Data audits; and (iv) Appointment of DPO. The DPA can require that any other data fiduciaries may have to undertake these obligations as well. **[Sections 33, 34, 35, 36 and 38 of the Bill]**

- The following enforcement tools shall be made available to the DPA: (i) Issuance of directions; (ii) Power to call for information; (iii) Publication of guidance; (iv) Issuance of public statement; (v) Codes of Practice; (vi) Conducting inquiry; (vii) Injunctive Relief; (viii) Inter-sectoral coordination. **[Chapter X of the Bill]**

- Pursuant to its powers of inquiry, the DPA has wide-ranging powers including issuing warnings, reprimands, ordering data fiduciaries to cease and desist, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law etc. **[Section 64 of the Bill]**

- The DPA's Adjudication Wing shall be responsible for adjudication of complaints between data principals and data fiduciaries. **[Section 68 of the Bill]**

- The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA. Appeals against orders of the appellate tribunal will be to the Supreme Court of India. **[Sections 84 and 87 of the Bill]**

- Penalties may be imposed on data fiduciaries and compensation may be awarded to data principals for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher. Offences created under the law should be limited to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. **[Sections 69, 70, 71, 72, 73, 75 and Chapter XIII of the Bill]**

SUMMARY OF RECOMMENDATIONS

Jurisdiction and Applicability

- The law will have jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. However, in respect of processing by fiduciaries that are not present in India, the law shall apply to those carrying on business in India or other activities such as profiling which could cause privacy harms to data principals in India. Additionally, personal data collected, used, shared, disclosed or otherwise processed by companies incorporated under Indian law will be covered, irrespective of where it is actually processed in India. However, the data protection law may empower the Central Government to exempt such companies which only process the personal data of foreign nationals not present in India. **[Sections 2 and 104 of the Bill]**
- The law will not have retrospective application and it will come into force in a structured and phased manner. Processing that is ongoing after the coming into force of the law would be covered. Timelines should be set out for notifications of different parts of the law to facilitate compliance. **[Section 97 of the Bill]**

Processing

- The definition of personal data will be based on identifiability. The DPA may issue guidance explaining the standards in the definition as applied to different categories of personal data in various contexts. **[Section 3(29) of the Bill]**

- The law will cover processing of personal data by both public and private entities. **[Sections 3(13) and 3(15) of the Bill]**

- Standards for anonymisation and de-identification (including pseudonymisation) may be laid down by the DPA. However, de-identified data will continue to be within the purview of this law. Anonymised data that meets the standards laid down by the DPA would be exempt from the law. **[Sections 3(3), 3(16) and 61(6)(m) of the Bill]**

- Sensitive personal data will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. However, the DPA will be given the residuary power to notify further categories in accordance with the criteria set by law. **[Sections 3(35) and 22 of the Bill]**

- Consent will be a lawful basis for processing of personal data. However, the law will adopt a modified consent framework which will apply a product liability regime to consent thereby making the data fiduciary liable for harms caused to the data principal. **[Section 12 of the Bill]**

- For consent to be valid it should be free, informed, specific, clear and capable of being withdrawn. For sensitive personal data, consent will have to be explicit. **[Sections 12 and 18 of the Bill]**

- A data principal below the age of eighteen years will be considered a child. Data fiduciaries have a general obligation to ensure that processing is undertaken keeping the best interests of the child in mind. Further, data fiduciaries capable of causing significant harm to children will be identified as guardian data fiduciaries. All data fiduciaries (including guardian data fiduciaries) shall adopt appropriate age verification mechanism and obtain parental consent. Furthermore, guardian data fiduciaries, specifically, shall be barred from certain practices. Guardian data fiduciaries exclusively offering counselling services or other similar services will not be required to take parental consent. **[Section 23 of the Bill]**

- The principle of granting protection to community data has been recognised by the Committee. This should be facilitated through a suitable law which is recommended to be enacted by the Government of India in the future.

Obligations of Data Fiduciaries

- The relationship between the "data subject" and the "data controller" is to be reformulated as a fiduciary relationship between the "data principal" and the "data fiduciary". **[Sections 3(13) and 3(14) of the Bill]**

- All processing of personal data by data fiduciaries must be fair and reasonable. **[Section 4 of the Bill]**

- The principles of collection and purpose limitation will apply on all data fiduciaries unless specifically exempted. **[Sections 5 and 6 of the Bill]**

- Processing of personal data using big data analytics where the purpose of the processing is not known at the time of its collection and cannot be reasonably communicated to the data principal can be undertaken only with explicit consent.

- A principle of transparency is incumbent on data fiduciaries from the time the data is collected to various points in the interim. Most prominently, a data fiduciary is obliged to provide notice to the data principal no later than at the time of the collection of her personal data. **[Sections 8 and 28 of the Bill]**

- There shall be obligations of data quality and storage limitation on data fiduciaries. However, the responsibility to ensure that the personal data provided is accurate will rest on the data principal. **[Sections 9 and 10 of the Bill]**

- There will be a provision of personal data breach notification to the DPA and in certain circumstances, to the data principal. **[Section 32 of the Bill]**

- Data security obligations will be applicable. **[Section 31 of the Bill]**

Data Principal Rights

- The right to confirmation, access and correction should be included in the data protection law. **[Sections 24 and 25 of the Bill]**

- The right to data portability, subject to limited exceptions, should be included in the law. **[Section 26 of the Bill]**

- The right to object to processing; right to object to direct marketing, right to object to decisions based on solely automated processing, and the right to restrict processing need not be provided in the law for the reasons set out in the report.

- The right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability on the basis of the five-point criteria as follows:

  (i) the sensitivity of the personal data sought to be restricted;
  (ii) the scale of disclosure or degree of accessibility sought to be restricted;
  (iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office);
  (iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public); and
  (v) the nature of the disclosure and the activities of the data fiduciary (whether the fiduciary is a credible source or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation). **[Section 27 of the Bill]**

- The right to be forgotten shall not be available when the Adjudication Wing of the DPA determines upon conducting the balancing test that the interest of the data principal in limiting the disclosure of her personal data does not override the right to freedom of speech and expression as well as the right to information of any other citizen. **[Section 27 of the Bill]**

- Time-period for implementing such rights by a data fiduciary, as applicable, shall be specified by the DPA. **[Section 28 of the Bill]**

Transfer of Personal Data outside India

- Cross border data transfers of personal data, other than critical personal data, will be through model contract clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. **[Section 41(1)(a) of the Bill]**

- Intra-group schemes will be applicable for cross-border transfers within group entities. **[Section 41(1)(a) of the Bill]**

- The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA. **[Section 41(1)(b) of the Bill]**

- Personal data determined to be critical will be subject to the requirement to process only in India (there will be a prohibition against cross border transfer for such data). The Central Government should determine categories of sensitive personal data which are critical to the nation having regard to strategic interests and enforcement requirements. **[Section 40(2) of the Bill]**

- Personal data relating to health will however be permitted to be transferred for reasons of prompt action or emergency. Other such personal data may additionally be transferred on the basis of Central Government approval. **[Section 41(3) of the Bill]**

- Other types of personal data (non-critical) will be subject to the requirement to store at least one serving copy in India. **[Section 40(1) of the Bill]**

Allied Laws

- Various allied laws are relevant in the context of data protection because they either require or authorise the processing of personal data for different objectives.

- All relevant laws will have to be applied along with the data protection law, as the latter will be the minimum threshold of safeguards for all data processing in the country. In the event of any inconsistency between data protection law and extant legislation, the former will have overriding effect.

- The proposed data protection framework replaces Section 43A of the IT Act and the SPD Rules issued under that provision. Consequently, these must be repealed together with consequent minor amendments. **[First Schedule of the Bill]**

- The RTI Act prescribes a standard for privacy protection in laying out an exemption to transparency requirements under Section 8(1)(j). This needs to be amended to clarify when it will be activated and to harmonise the standard of privacy employed with the general data protection statute. **[Second Schedule of the Bill]**

- The Committee has identified a list of 50 statutes and regulations which have a potential overlap with the data protection framework. Concerned ministries may take note of this and ensure appropriate consultation to make complementary amendments where necessary.

- The Aadhaar Act needs to be amended to bolster data protection. Suggested amendments for due consideration are contained in the Appendix to this Report.

Non-Consensual Grounds of Processing

- Functions of the State: Welfare functions of the state will be recognised as a separate ground for processing. Processing activities carried out by the State under law will be covered under this ground, ensuring that it is in furtherance of public interest and governance. However, only bodies covered under Article 12 of the Constitution may rely on this ground. Processing towards activities that may not be considered part of a welfare functions would, however, not to be permitted. Thus, the availability of this ground is restricted to certain entities and certain functions to avoid vagueness in the law. **[Sections 13 and 19 of the Bill]**

- Compliance with Law or Order of Court or Tribunal: Compliance with law or order of court or tribunal will be recognised as a separate ground for processing to avoid inconsistency with obligations under other laws, regulations and judicial orders. The word 'law' shall be construed to mean laws, ordinances, orders, bye-law, rules, regulations and notifications that have statutory authority. Order of court or tribunal would be restricted to Indian courts and tribunals. Obligations imposed by contract, foreign law and foreign judicial orders shall not be permitted to be processed under this ground. **[Sections 14 and 20 of the Bill]**

- Prompt Action: Prompt action will be recognised as a separate ground for processing. It should receive a strict interpretation and only be applied in critical situations where the individual is incapable of providing consent and the processing is necessary to meet emergency situations. **[Sections 15 and 21 of the Bill]**

- Employment: Employment will be recognised as a separate ground for processing. This ground should be invoked only where processing under consent would involve disproportionate effort or where the employment relation makes consent inappropriate, and will permit processing even where employment-related activities are not authorised under any of the other grounds of processing such as compliance with law. **[Sections 16 of the Bill]**

- Reasonable Purpose: Reasonable purpose is a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action and public function but are still useful to society. The ambit of the provision would be limited to those purposes which are whitelisted by the DPA to guide data fiduciaries. **[Section 17 of the Bill]**

Exemptions

- Security of the State: The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is necessary in the interest of the security of the state. Any restriction must be proportionate and narrowly tailored to the stated purpose. The Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities. **[Section 42 of the Bill]**

- Prevention, Detection, Investigation and Prosecution of Contraventions of Law: The data protection law should provide an exemption for prevention, detection, investigation and prosecution of contraventions of law (including protection of revenue). In order to invoke the exemption, the law enforcement agencies must be authorised by law. **[Section 43 of the Bill]**

- Disclosure for the Purpose of Legal Proceedings: The disclosure of personal data necessary for enforcing a legal right or claim, for seeking any relief, defending any charge, opposing any claim or for obtaining legal advice from an advocate in an impending legal proceeding would be exempt from the application of the data protection law. General obligations of security and fair and reasonable processing will continue to apply. **[Section 44 of the Bill]**

- Research Activities: The research exemption is not envisaged as a blanket exemption. Only those obligations that are necessary to achieve the object of the research will be exempted by the DPA. This assessment is contextual and dependent on the nature of the research. **[Section 45 of the Bill]**

- Personal or Domestic Purposes: A narrowly tailored exemption for purely personal or domestic processing of data should be incorporated in the data protection law. It would provide a blanket exemption from the application of the data protection law. **[Section 46 of the Bill]**

- Journalistic Activities: To strike a balance between freedom of expression and right to informational privacy, the data protection law would need to signal what the term 'journalistic purposes' signifies, and how ethical standards for such activities would need to be set. Where these conditions are met, an exemption should be provided. **[Section 47 of the Bill]**

- Manual Processing by Small Entities: Since the risk of privacy harms being caused are higher when personal data is processed through automated means, an exemption will be made in the data protection law for manual processing by data fiduciaries that are unlikely to cause significant harm and would suffer the heaviest relative burdens from certain obligations under this law. **[Section 48 of the Bill]**

Enforcement

- The data protection law will set up a DPA which will be an independent regulatory body responsible for the enforcement and effective implementation of the law. Broadly, the DPA shall perform the following primary functions: (i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (iv) inquiry, grievance handling and adjudication. **[Chapter X of the Bill]**

- The DPA is vested with the power to categorise certain fiduciaries as significant data fiduciaries based on their ability to cause greater harm to data principals as a consequence of their data processing activities. This categorisation will be based on an assessment of volume of the personal data being processed, nature of personal data, type of processing activity undertaken, turnover of the data fiduciary, the risk of harm, and the type of technology used to undertake processing. **[Section 38 of the Bill]**

- Significant data fiduciaries will have to undertake obligations such as: (i) Registration with the DPA; (ii) Data Protection Impact Assessments; (iii) Record-keeping; (iii) Data audits; and (iv) Appointment of DPO. The DPA can require that any other data fiduciaries may have to undertake these obligations as well. **[Sections 33, 34, 35, 36 and 38 of the Bill]**

- The following enforcement tools shall be made available to the DPA: (i) Issuance of directions; (ii) Power to call for information; (iii) Publication of guidance; (iv) Issuance of public statement; (v) Codes of Practice; (vi) Conducting inquiry; (vii) Injunctive Relief; (viii) Inter-sectoral coordination. **[Chapter X of the Bill]**

- Pursuant to its powers of inquiry, the DPA has wide-ranging powers including issuing warnings, reprimands, ordering data fiduciaries to cease and desist, modify or temporarily suspend businesses or activities of data fiduciaries who are found to be in contravention of the law etc. **[Section 64 of the Bill]**

- The DPA's Adjudication Wing shall be responsible for adjudication of complaints between data principals and data fiduciaries. **[Section 68 of the Bill]**

- The Central Government shall establish an appellate tribunal or grant powers to an existing appellate tribunal to hear and dispose of any appeal against an order of the DPA. Appeals against orders of the appellate tribunal will be to the Supreme Court of India. **[Sections 84 and 87 of the Bill]**

- Penalties may be imposed on data fiduciaries and compensation may be awarded to data principals for violations of the data protection law. The penalties imposed would be an amount up to the fixed upper limit or a percentage of the total worldwide turnover of the preceding financial year, whichever is higher. Offences created under the law should be limited to any intentional or reckless behaviour, or to damage caused with knowledge to the data principals in question. **[Sections 69, 70, 71, 72, 73, 75 and Chapter XIII of the Bill]**

No. 3(6)/2017-CLES
Government of India
Ministry of Electronics & Information Technology

Electronics Niketan
New Delhi-110003
Dated : 31st July, 2017

OFFICE MEMORANDUM

Subject: Constitution of a Committee of Experts to deliberate on a data protection framework for India

The Government of India is cognizant of the growing importance of data protection in India. The need to ensure growth of the digital economy while keeping personal data of citizens secure and protected is of utmost importance.

2. It has thus been decided to constitute a Committee of Experts under the Chairmanship of Justice B N Srikrishna, Former Judge, Supreme Court of India, to identify key data protection issues in India and recommend methods of addressing them. The constitution of the group and terms of reference are as follows:

a) Justice B N Srikrishna, Former Judge, Supreme Court of India	- Chairperson
b) Smt. Aruna Sundararajan, Secretary, Department of Telecom	- Member
c) Dr Ajay Bhushan Pandey, CEO,UIDAI	- Member
d) Dr Ajay Kumar, Addl Secretary, MeitY	- Member
e) Prof Rajat Moona, Director, IIT, Raipur	- Member
f) Dr. Gulshan Rai, National Cyber Security Coordinator	- Member
g) Prof. Rishikesha T. Krishnan, Director, IIM, Indore	- Member
h) Dr. Arghya Sengupta, Research Director, Vidhi Centre for Legal Policy	- Member
i) Ms. Rama Vedashree, CEO, DSCI	- Member
j) Joint Secretary, MeitY	- Member Convener

3. **Terms of Reference**

a) To study various issues relating to data protection in India
b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill.

Contd...2/-

4. The Committee may co-opt other members in the Group for their specific inputs.

5. MeitY shall in consultation with the Chairperson and members, collect necessary information and provide it to the Committee within 8 weeks of the date of this OM to enable it to start its deliberations on the subject.

6. The Committee shall endeavour to submit its report as expeditiously as possible.

7. The expenditure towards TA/DA in connection with the meetings of the group in respect of the official members will be borne by their respective Ministries/Departments. Domestic travel in respect of non-official members would be permitted by Air India (Business Class) and the expenditure would be met by MeitY.

(Rakesh Maheshwari)
Group Coordinator,
Cyber Law & UIDAI

To

1) Justice B N Srikrishna, Former Judge Supreme Court of India
2) Smt. Aruna Sundararajan, Secretary,
3) Dr Ajay Bhushan Pandey, CEO,UIDAI
4) Dr Ajay Kumar, Addl Secretary, MeitY
5) Prof Rajat Moona, Director, IIT, Raipur
6) Dr. Gulshan Rai, National Cyber Security Coordinator
7) Prof. Rishikesha T. Krishnan, Director, IIM, Indore
8) Dr. Arghya Sengupta, Research Director, Vidhi Centre for Legal Policy
9) Ms. Rama Vedashree, CEO, DSCI
10) Joint Secretary, MeitY

Copy to:
i) PS to Hon'ble, Minister (E&IT)
ii) PS to Hon'ble MoS (E&IT)
iii) OSD to Secretary, MeitY
iv) All Group Coordinators, MeitY

How can Privacy Policy documents be designed for better communication?

These suggestions have been arrived at after studying Privacy Policy documents of over twenty platforms, including online marketplaces, search engines, social networks, etc. Their chief objective is to improve the presentation of these textual documents, making them easier to consume and understand.

These suggestions will each improve these documents along one or more of the following parameters:

APPROACHABILITY
Minimising the intimidating nature of such documents, to encourage engagement

COMPREHENSIBILITY
Simplifying and organising the content to make it more easily and widely understandable

HELPFULNESS
Making the text an active assistant in engagement and comprehension, and not just a passive vehicle for the content

LEGIBILITY & READABILITY
Optimising the typography and page layout for easy and effortless perusal

CONSCIENTIOUSNESS
Prioritising users' right to be informed about their data and its use, and giving them granular control over what they consent to.

One
Simplifying Text

- Simplify phrasing, with crisp sentences and easier words.
- Rephrase section headings as questions.

EXAMPLES:

We use the information we collect to show you content that's relevant, interesting and specific to you. Here's how:

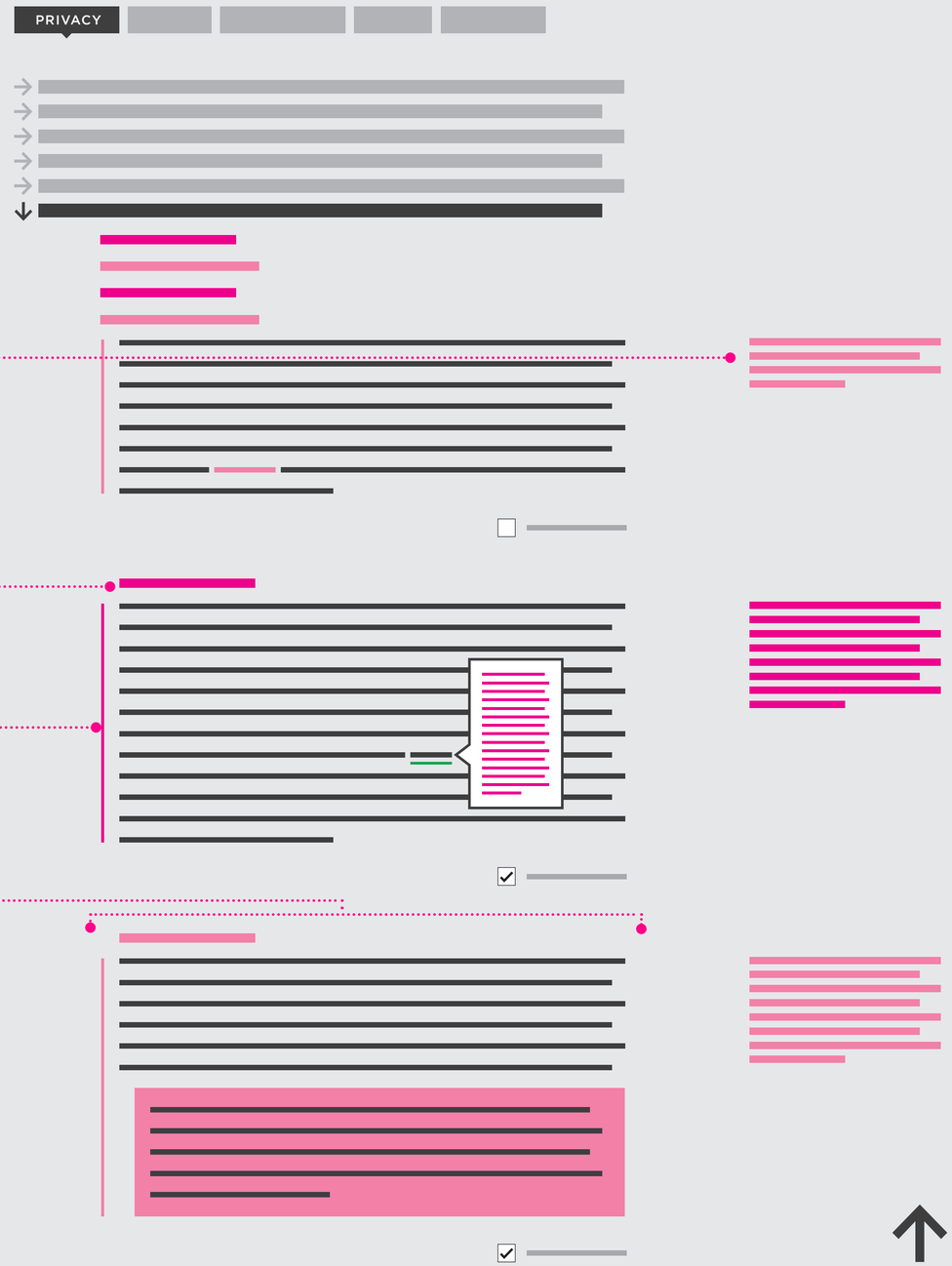
Who has access to my information?

Two
Structuring Content, with Intuitive Navigation

- Provide a separate page for all Privacy-related information, as a distinct tab.
- Categorise the content into sections, as a collapsible list of links.
- Segregate content within a section into sub-sections, wherever possible, as a collapsible list of links.
- Provide intra- or inter- document links, when a reference to a different section within the Privacy Policy document, or in another document, is made.
- Collapse tangential, instantial or incidental information into mouse-over or pop-up links.
- User input fields (for permissions) should be opt-in, instead of opt-out, (for instance: no pre-checked boxes).
- These requests for permissions should be de-bundled, with separate input fields appearing alongside the clause relevant to them.
- Provide a link to return to the top of the page, at all points of scrolling.

Three
Designing for Ease (Macro)

- Supply a brief, plain-language summary beside each section, with the salient points of the section. This would be non-binding, and only intended as an aid.
- Use non-textual design elements, such as icons, colour codes etc.—strategically, to aid meaning.
- Fix column widths at 55-65 characters (including spaces), leaving generous amounts of white space on all sides of the text column(s), as far as possible.



Four
Designing for Ease (MIcro)

- Use a font which is easily legible.
- Provide adequate line spacing.
- Differentiate between different types of text (section headings, sub-section headings, body text etc.) such that they are immediately distinguishable from one another. This can be done through:
  - Font attributes: create clear differences in weight, size and colour
  - Positioning: increase distance from dissimilar content, decrease distance from similar content, create visual ‘clubs’
  - Lists: use ordered or unordered lists, wherever possible.
- Use typographic treatment consistently—the same kind of content must have the same appearance throughout the document.

Five
Creating Emphasis (for Disclaimers, Onerous Clauses etc.)

- Use proper capitalisation—avoid all-uppercase.
- Create, and consistently follow, a visual style for emphasis that is instantly noticeable, without compromising on readability. Outlined below are a few ways to achieve that:
  - Visual markers: Fields of colour, icons, etc.
  - Font attributes: differentiate from body text in weight, size and/or colour.
  - Positioning: break alignment from the rest of the text, to draw attention.

EXAMPLE:

What information do we collect?

When you sign up for or use <Example>, you give us certain information voluntarily. This includes your name, email address, phone number, profile photo, comments, and any other information you give us. You can also choose to share with us location data or photos.

If you link your Facebook or Google account or accounts from other third party services to Pinterest, we also get information from those accounts (such as your friends or contacts). The information we get from those services depends on your settings and their privacy policies, so please check what those are.

<Example> may contain links to other sites. <Example> is not responsible for the privacy policies and/or practices on other sites. When linking to another site you should read the privacy policy stated on that site. This Privacy Policy only governs information collected by <Example>.

Six
Providing language support

Provide options to view the document in the common languages of the regions where the service is available.

Seven
Optimising across Devices

Design for common break-points, ensuring maximum reader-friendliness across all common devices.

Eight
Providing for Offline Use

Supply an offline version of the document—if the original privacy policy is provided online—with the same content organisation, hierarchy and typographic treatment.

Nine
Presenting in Other forms

While all the above suggestions are for textual documents, platforms are also encouraged to arrive at audio-visual ways in which Privacy Policies can be explained. This would greatly aid user engagement and comprehension.

ANNEXURE C

List of Allied Laws Impacted by a Draft Data Protection Law in India

A. Information Technology Laws

1. Indian Telegraph Act, 1885
2. Information Technology Act, 2000
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules, 2011

B. Land and Taxation Laws

1. The Right to Fair Compensation and Transparency in Land Acquisition Act, 2013
2. Income Tax Act, 1961
3. Central Goods and Services Tax Act, 2017
4. The Black Money (Undisclosed Foreign Income and Assets) And Imposition of Tax Act, 2015

C. Criminal Justice Laws

1. Prisons Act, 1894
2. Identification of Prisoners Act 1920
3. Official Secrets Act, 1923

D. Law relating to International Relations

1. United Nations (Privileges and Immunities) Act, 1947

E. Alternative Dispute Resolution

1. The Arbitration and Conciliation Act, 1996

F. Health Laws

1. The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
2. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994
3. The Mental Health Act, 1987
4. Persons with Disabilities (Equal Opportunities, Protection of Rights and Full Participation) Act, 1995

G. Intellectual Property Laws

1. Trademarks Act, 1999
2. Copyright Act, 1957

H. Symbols, Records and Statistics Laws

1. The Collection of Statistics Act, 2008
2. The Census Act, 1948

I. Trade and Commerce Laws

1. Bureau of Indian Standards Act, 1986

J. Defence Laws

1. The Enemy Property Act, 1968
2. The Defence of India Act, 1962

K. Labour and Employment Laws

1. The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013
2. Employees' Provident Fund and Miscellaneous Provisions Act, 1952
3. Employees' State Insurance Act, 1948

L. Corporate and Financial Laws

1. Reserve Bank of India Act, 1935
2. Insurance Act, 1938
3. Banking Regulation Act, 1934
4. National Bank for Agriculture and Rural Development Act, 1981
5. National Housing Bank, 1987
6. Small Industries and Development Bank of India Act, 1989
7. Payment and Settlement Systems Act, 2007
8. Depositories Act, 1996
9. Companies Act, 2013
10. Insolvency and Bankruptcy Code, 2016
11. Securities & Exchange Board of India Act, 1992
12. Competition Act, 2002
13. Securities Contracts (Regulation) Act
14. Credit Information Companies (Regulation) Act, 2005
15. Limited Liability Partnership Act, 2008
16. Prevention of Money Laundering Act, 2002

M. Miscellaneous

1. The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016
2. Consumer Protection Act, 1986
3. Right of Children to Free and Compulsory Education Act, 2009
4. Right to Information Act, 2005
5. The Telecom Regulatory Authority of India Act, 1997
6. Foreign Contribution (Regulation) Act, 2010
7. The Prohibition of Benami Property Transactions, 1988
8. Indian Evidence Act, 1872

APPENDIX

Suggested amendments to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

The following amendments have been suggested to the Aadhaar Act from a data protection perspective. They must be read alongside Chapters XI and XII of the proposed data protection bill which deal with enforcement action and individual remedies. The rationale for these amendments have been explained in the Report from pages 98 to 101. The amendments may be duly considered by the Government and suitable legislation introduced as deemed appropriate.

1. **Amendment of section 2. —** In section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (hereinafter referred to as the principal Act),

(1) in place of the current clause (a), the following clause shall be substituted, namely:—

"(a) "Aadhaar number" means a twelve-digit identification number issued to an individual under sub-section (3) of section 3 and includes any alias thereof generated in a manner specified by regulations"

(2) after clause (b), the following clauses shall be inserted, namely:—

"(ba) "Adjudicating Officer" means an adjudicating officer appointed under sub-clause (1) of section 33B;"

"(bb) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;"

(3) after clause (m), the following clause shall be inserted, namely:—

"(ma) "Entities in the Aadhaar ecosystem" includes enrolling agencies, Registrars, requesting entities, offline verification-seeking entities and any other entity or group of entities as specified by the Authority;"

(4) after clause (p), the following clauses shall be inserted, namely:—

"(pa) "Offline verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;"

"(pb) "Offline verification-seeking entity" means any entity desirous of undertaking offline verification of an Aadhaar number holder."

2. Amendment of section 4.— In place of the current sub-section (3) of section 4 of the principal Act, the following sub-section (3) of section 4 shall be substituted, namely:—

"(3) An Aadhaar number, in physical or electronic form subject to authentication or offline verification and other conditions, as may be specified by regulations, may be accepted as proof of the identity of the Aadhaar number holder for any purpose."

3. Amendment of section 8.— (1) In place of sub-section (1) of section 8 of the principal Act, the following sub-sections shall be substituted, namely:—

"8. Authentication of Aadhaar number .—

(1) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder on the request of a requesting entity only when such authentication is:

(a) mandated pursuant to law made by Parliament;
(b) required by a public authority for performing a public function, subject to prior approval of the Authority on such conditions as the Authority may deem fit.

(1A) In determining whether to grant approval under sub-section (1), the Authority shall take into account the following factors:

(a) the nature of the interest of the requesting entity seeking authentication;
(b) the standards of security employed by the requesting entity; and
(c) any other factor which is relevant in protecting the privacy of an Aadhaar number holder.

(1B) The Authority may, by regulations, classify requesting entities into such categories as may be necessary to determine whether such requesting entity may request an Aadhaar number holder for the Aadhaar number itself during authentication or only any alias or aliases thereof."

(2) After clause (b) of sub-section (2) of section 8 of the principal Act, the following clause shall be inserted, namely: —

"(c) ensure the availability of alternate and viable means of identification of an Aadhaar number holder in case of a failure to authenticate on account of

illness, injury or infirmity owing to old age or otherwise, and any technical reasons as may be specified."

4. Insertion of section 8A.— After section 8 of the principal Act, the following section 8A shall be inserted, namely:—

"(8A) Offline verification of Aadhaar number.—

(1) Any offline verification of an Aadhaar number holder shall take place on the basis of consent provided to such verification by the Aadhaar number holder.

(2) Any offline verification-seeking entity shall,

(a) obtain the consent of an individual before verifying him offline, in such manner as may be specified by regulations; and

(b) ensure that the demographic information or any other information collected from the individual for offline verification, if any, is only used for the purpose of such verification.

(3) An offline verification-seeking entity shall inform the individual undergoing offline verification the following details with respect to offline verification, in such manner as may be specified by the regulations, namely: —

(a) the nature of information that may be shared upon offline verification;

(b) the uses to which the information received during offline verification may be put by the offline verification requesting entity;

(c) alternatives to submission of information requested for, if any.

(4) An offline verification-seeking entity shall not:

(a) subject an Aadhaar number holder to authentication;

(b) collect, use or store an Aadhaar number or biometric information of any individual for any purpose;

(c) take any action contrary to any obligations on it, specified by regulations.

5. Substitution of section 21.— In place of the current section 21 of the principal Act, the following section 21 shall be substituted, namely:—

"**21. Officers and other employees of Authority.—**

(1) The Authority shall determine the number, nature and categories of other officers and employees required for the discharge of its functions under this Act.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and other employees of the Authority shall be such, as may be specified."

6. Amendment of section 23.— After section 23 of the principal Act, the following sections shall be inserted, namely:—

"**23A. Power of Authority to issue directions.—**

(1) The Authority may, in exercise of its powers or for discharge of its functions under this Act, or any rules or regulations made hereunder, issue such directions from time to time to entities in the Aadhaar ecosystem, as it may consider necessary.

(2) Any direction issued under sub-section (1) for providing alternate and viable means of identification in case of failure to authenticate shall have effect, notwithstanding anything contained in any law in force.

(3) If the Authority finds, on the basis of material in its possession, that any person has violated, or is likely to violate, any provisions of this Act, or any rules or regulations made thereunder, it may pass an order requiring such person to cease and desist from committing or causing such violation, or give such directions as may be necessary for the purpose of securing compliance with that condition or provision."

"23B. Power of Authority to conduct inquiry.—

(1) The Authority may conduct an inquiry where it has reasonable grounds to believe that—

(a) the activities of an entity in the Aadhaar ecosystem are being conducted in a manner which is detrimental to, or in violation of the privacy of an individual or an Aadhaar number holder; or

(b) any entity in the Aadhaar ecosystem has violated any of the provisions of this Act or the rules prescribed or the regulations specified or directions issued by the Authority thereunder.

(2) For the purpose of sub-section (1), the Authority shall, by an order in writing, appoint an Inquiry Officer to conduct the inquiry where such order shall set out inter alia the scope of inquiry and reasons for commencing inquiry and the Inquiry Officer shall prepare an inquiry report to be submitted to the Authority.

(3) Every person acting under the direct authority of the entity in the Aadhaar ecosystem, service provider or a contractor where services are being obtained by or provided to the entity in the Aadhaar ecosystem, as the case may be, shall be bound to produce before the Inquiry Officer,

all such documents, records and data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the entity in the Aadhaar ecosystem as the Inquiry Officer may require within the time stipulated by such officer.

(4) The Inquiry Officer shall undertake the inquiry only after providing a written notice to the persons referred to in sub-section (3) stating the reasons for the inquiry and the relationship between the entity in the Aadhaar ecosystem and the scope of the investigation.

(5) The Inquiry Officer may keep in its custody any documents, records and data referred to in sub-section (3) for six months and thereafter shall return the same to the persons concerned.

(6) Without prejudice to the provisions of this Act or any other law, an Inquiry Officer may examine on oath, any person acting under the direct authority of the entity in the Aadhaar ecosystem, or a service provider, or a contractor where services are being obtained by or provided to the entity in the Aadhaar ecosystem, as the case may be, for conducting an inquiry.

"23C. Powers of Search and Seizure.—

(1) Where the Authority has reasonable grounds to believe that—

(a) any person referred to in sub-section (3) of section 23B has failed or omitted to produce any documents, records or data in her custody or power; or

(b) any such documents, records or data mentioned in clause (a) of sub-section (1) are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed; or

(c) a contravention of any provision of this Act has been committed or is likely to be committed by an entity of the Aadhaar ecosystem,

it may authorise any officer of the Authority not below the rank equivalent to that of a Gazetted Officer of the Central Government (hereinafter referred to as "Authorised Officer") to—

(i) enter and search any building or place where she has reason to suspect that such documents, records or data are kept;

(ii) break open the lock of any box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (i) where the keys thereof are not available;

(iii) access any computer, computer resource, or any other device containing or suspected to be containing data;

(iv) seize all or any such documents, records or data found as a result of such search;

(v) place marks of identification on such documents, records or databases or make extracts or copies of the same.

(2) The Authorised Officer may requisition the services of any police officer or of any officer of the Central Government, or of both, as the case may be, for assistance related to any of the purposes specified in sub-section (1) and it shall be the duty of every such officer to comply with such requisition.

(3) The Authorised Officer may, where it is not practicable to seize any such document, record or data specified in sub-section (1), serve an order on the person who is in immediate possession or control thereof that such person shall not remove, part with or otherwise deal with it except with the previous permission of such officer.

(4) The Authorised Officer may, during the course of the search or seizure, examine on oath any person who is found to be in possession or control of any documents, records or data, and any statement made by such person during such examination may thereafter be used in evidence in any proceeding under this Act.

(5) The documents, records or data seized under sub-section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the approval of the Authority for such retention is obtained.

(6) The Authority shall not authorise the retention of documents, records or data for a period exceeding thirty days after all the proceedings under this Act, for which the said documents, records or data are relevant, are completed.

(7) The person from whose custody the documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer at such place and time as may be designated.

(8) If a person legally entitled to the documents, records or data seized under sub-section (1) objects for any reason to the approval given by the Authority under sub-section (5), such person may make an application to the Appellate Tribunal stating her objection and requesting for the return of the same.

(9) On receipt of the application under sub-section (8), the Appellate Tribunal may, after giving the parties an opportunity of being heard, pass such order as it thinks fit.

(10) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) relating to searches and seizures shall apply, so far as may be, to every search and seizure made under sub-section (1).

(11) Without prejudice to the generality of the foregoing, rules may be prescribed in relation to the process for search and seizure under this section as may be deemed fit by the Authority.

"23D. Action to be taken by Authority pursuant to an inquiry.—

(1) On receipt of a report under sub-section (2) of section 23B, the Authority may, after giving such opportunity to the entity in the Aadhaar ecosystem

to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—

(a) issue a warning to the entity in the Aadhaar ecosystem where the business or activity is likely to violate the provisions of this Act;
(b) issue a reprimand to the entity in the Aadhaar ecosystem where the business or activity has violated the provisions of this Act;
(c) require the entity in the Aadhaar ecosystem to cease and desist from committing or causing any violation of the provisions of this Act;
(d) require the entity in the Aadhaar ecosystem to modify its business or activity to bring it in compliance with the provisions of this Act;
(e) temporarily suspend or discontinue business or activity of the entity in the Aadhaar ecosystem which is in contravention of the provisions of this Act;
(f) initiate proceedings under section 33A of this Act;
(g) make a complaint under section 47 of this Act;
(h) require the entity in the Aadhaar ecosystem to take any such action in respect of any matter arising out of the report as the Authority may think fit.
(i) issue any other direction as it deems fit under sub-section (3) of section 23A of this Act;

(2) An entity in the Aadhaar ecosystem aggrieved by an order made under this section by the Authority, except an order under clause (f) and (g) of sub-section (1), may prefer an appeal to the Appellate Tribunal."

7. In place of the current section 25 of the principal Act, the following section shall be substituted, namely:—

"**25. Other fees and revenues.**—

The fees or revenue collected by the Authority shall be credited to a fund called the Unique Identification Authority of India Fund to be managed by the Authority."

8. In place of the current sub-section (4) of section 29 of the principal Act, the following sub-section (4) shall be substituted, namely:—

"**29. Restriction on sharing information.**—

(4) No Aadhaar number, demographic information or photograph collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for purposes, if any, as may be specified.

Provided, nothing in this sub-section shall apply to core biometric information which shall only be governed by sub-section (1).”

9. Insertion of Chapters after Chapter VI.—After Chapter VI of the principal Act, the following Chapters shall be inserted, namely:—

“**CHAPTER VIA**
CIVIL PENALTIES

33A. Penalty for failure to comply with provisions of this Act, rules, regulations and directions.—

Whoever fails to comply with any provision of this Act, the rules or the regulations made hereunder or directions issued by the Authority under the provisions of this Act, or fails to furnish any information, document, or return of report required by the Authority, shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

33B. Power to adjudicate.—

(1) For the purposes of adjudication under section 33A and imposing a penalty thereunder, the Authority shall appoint any officer, not below the rank of a Joint Secretary to the Government of India, to be an Adjudicating Officer for adjudicating disputes in the manner prescribed by the Central Government.

(2) The proceedings under sub-section (1) can only be initiated by the Authority against entities in the Aadhaar ecosystem.

(3) While conducting the proceedings the Adjudicating Officer shall, —

(a) provide the entities in the Aadhaar ecosystem against whom a penalty is proposed to be levied, an oral hearing;

(b) have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the proceedings.

(4) Based on the information received pursuant to sub-section (3), if the Adjudicating Officer is satisfied that any entity in the Aadhaar ecosystem has failed to comply with any provision of this Act, the rules or the regulations made hereunder or directions issued by the Authority under the provisions of this Act, or has failed to furnish any information, document, or return of report required by the Authority, the Adjudicating Officer may, by order, impose such

penalty as he thinks fit in accordance with the provisions of section 33A.

(5) Every Adjudicating Officer shall have the powers of a civil court, for the purposes of—

(a) Sections 193 and 228 of the Indian Penal Code, 1860;
(b) Sections 345 and 346 of the Code of Criminal Procedure, 1973;
(c) Order XXI of the Code of Civil Procedure, 1908.

CHAPTER VIB
APPEALS

33C. Appeals to Appellate Tribunal.—

(1) Any person aggrieved by an order passed by an Adjudicating Officer under sub-section (4) of section 33B, may prefer an appeal before the Appellate Tribunal.

(2) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date of receipt of the order appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.

(3) On receipt of an appeal under sub-section (1), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the Adjudicating Officer.

(5) Any appeal filed under sub-section (1) shall be dealt with by the Appellate Tribunal as expeditiously as possible and every endeavour shall be made by it to dispose of the appeal within six months from the date on which it is presented to it.

(6) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness of any order or decision of the Adjudicating Officer, either on its own motion or otherwise, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

33D. Procedure and powers of the Appellate Tribunal.—

The provisions of sections 14I to 14K (both inclusive), 16 and 17 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) shall *mutatis mutandis* apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under the Telecom Regulatory Authority of India Act, 1997 (24 of 1997).

33E. Orders passed by Appellate Tribunal to be executable as a decree.—

(1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of a civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

33F. Penalty for willful failure to comply with orders of Appellate Tribunal.—

If any person willfully fails to comply with the order of the Appellate Tribunal, he shall be punishable with a fine which may extend to one lakh rupees, and in case of a second or subsequent offence with a fine which may extend to two lakh rupees, and in the case of continuing contravention with an additional fine which may extend to two lakh rupees for every day during which such default continues.

33G. Appeal to Supreme Court.—

(1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order, not being an interlocutory order, of the Appellate Tribunal to the Supreme Court only if it raises a substantial question of law.

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal which the parties have consented to.

(3) Every appeal under this section shall be preferred within a period of forty-five days from the date of the decision or order appealed against.

33H. Recovery of penalty or compensation.—

(1) For the purpose of this Act, the Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer who shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.

(2) Where any person fails to comply with— an order of the Adjudicating Officer imposing a penalty under the provisions of this Act, the Recovery Officer may recover from such person the aforesaid amount in any of the following ways, in descending order of priority, namely—

(a) attachment and sale of the person's movable property;

(b) attachment of the person's bank accounts;
(c) attachment and sale of the person's immovable property;
(d) arrest and detention of the person in prison;
(e) appointing a receiver for the management of the person's movable and immovable properties.

(3) For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the said provisions and rules—

(a) were the provisions of this Act; and
(b) referred to the amount due under this Act instead of to income tax under the Income Tax Act, 1961 (43 of 1961).

(4) In this section, the movable or immovable property or monies held in a bank account shall include property or monies which meet all the following conditions—

(a) property or monies transferred by the person without adequate consideration;
(b) such transfer is made:

(i) on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and
(ii) to the person's spouse, minor child, son's wife or son's minor child.

(c) such property or monies are held by, or stand in the name of, any of the persons referred to in sub-clause (b), including where they are so held or stand in the name of such persons after they have attained the age of majority.

33I. Civil Court not to have jurisdiction.—

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an Adjudicating Officer appointed under this Act or the Appellate Tribunal is empowered, by or under this Act to determine, and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."

10. Amendment of sections 38 and 39.— In sections 38 and 39 of the principal Act, for the words "imprisonment for a term which may extend to three years", the

words "imprisonment for a term which may extend to ten years" shall be substituted.

11. Substitution of section 40.— In place of the current section 40 of the principal Act, the following section 40 shall be substituted, namely:—

"**40. Penalty for unauthorised use by requesting entity**.—

Whoever, being a requesting entity, fails to obtain the consent of an individual before collecting his identity information for the purposes of authentication in contravention of clause (a) of sub-section (2) of Section 8, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both."

12. Insertion of sections 41A, 41B, 41C, 41D.— After section 41 of the principal Act, the following sections shall be inserted, namely:—

"41A. Penalty for failure to obtain consent for authentication or offline verification.—

Whoever, being a requesting entity or an offline verification seeking entity, fails to obtain the consent of an individual before collecting his identity information for the purpose of authentication in contravention of clause (a) of sub-section (2) of Section 8, or necessary information for the purpose of offline verification in contravention of clause (a) of sub-section (2) of section 8A, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.

41B. Penalty for unauthorised use of core biometric information.—

Whoever uses core biometric information collected or created under this Act for any purpose other than generation of Aadhaar numbers and authentication under this Act, shall be punishable with imprisonment which shall not be less than three years but which may extend to ten years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to fifty lakh rupees, or with both.

41C. Penalty for unauthorised publication of Aadhaar number or photograph.—

Whoever wrongfully publishes, displays or posts publicly, Aadhaar numbers collected or created under this Act, or demographic information or photograph in respect of an Aadhaar number holder, except for the

purposes specified under this Act or regulations, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both."

41D. Penalty for offline verification-seeking entities.—

Whoever, being an offline verification-seeking entity, collects, stores or uses the Aadhaar number of an Aadhaar number holder or makes an Aadhaar number holder undergo authentication, unless mandated pursuant to any law enacted by Parliament, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both."

13. Amendment of section 42.— In section 42 of the principal Act, for the words "imprisonment for a term which may extend to one year", the words "imprisonment for a term which may extend to three years" shall be substituted.

14. Amendment of section 53.— In section 53, in sub-section (2), —

(1) after clause (d), the following clauses shall be added, namely:—

"(da) the process for search and seizure under sub-section (11) of section 23C;"

(2) In section 53, in sub-section (2), after clause (g), the following clauses shall be added, namely:—

"(ga) the manner of appointment of an adjudicating officer under sub-section (1) of section 33B;"

"(gb) the form, manner, and fee for an appeal to be filed under sub-section (2) of section 33C."

15. Amendment of section 54.— In section 54 of the principal Act, in sub-section (2),

(1) after clause (a), the following clauses shall be added, namely :—

"(aa) the manner of generating an alias of Aadhaar under clause (a) of section 2;"

"(ab) the entities or group of entities in the Aadhaar ecosystem under clause (ma) of section 2;"

"(ac) the modes of offline verification of Aadhaar number under clause (pa) of section 2;"

(2) after clause (f), the following clauses shall be added, namely :—

"(fa) the classification of requesting entities under sub-section (1B) of section 8;"

"(fb) the technical reasons necessitating the specification of alternate and viable means of identification under clause (c) of sub-section (2) of Section 8;"

"(fc) the manner of obtaining consent under clause (a) of sub-section (2) of section 8A;"

"(fd) the manner of providing information to the individual undergoing offline verification under clause sub-section (3) of section 8A;"

"(fd) the obligations of offline verification-seeking entities under clause (c) of sub-section (4) of section 8A;"

(3) after clause (u), the following clauses shall be added, namely :—

"(ua) the purposes for which Aadhaar number, demographic information or photograph collected may be published, displayed or posted publicly under sub-section (4) of Section 29;"

16. Amendment of section 57.— In the proviso to section 57 of the principal Act, after the words "under section 8" the following words and numbers shall be inserted namely :—

", section 8A"

Vikash

From: Rama Vedashree (DSCI) [rama@dsci.in]
Sent: Friday, July 27, 2018 2:37 PM
To: js.gopal@meity.gov.in; Srikrishna BN
Cc: Ajay Sawhney; Vikash Chourasia
Subject: My Note on the final Version of Draft Bill received on 26th July 2018
Attachments: Dissent Note Rama Vedashree.docx; Copy of Sensitive Personal Data Final.xlsx

Dear Sirs

I wish to thank you both for giving me the opportunity to participate in the Committee Deliberations, and giving me a patient hearing in all the meetings and submissions, during the last one year.

It has been a tremendous learning for me to participate in the meetings and learn from all the committee members and the chair.

Iam fully supportive of Govt bringing a strong Data Protection and Privacy regime. Data Security Council of India (A NASSCOM Initiative) owes its genesis to driving best practices in Data Protection comparable with global models in the Industry. We have pioneered a Privacy Framework, and Credentials and Certification Program namely DSCI Privacy Framework and DCPP, DCPLA, which is widely adopted by Industry members across IT, Banking and Telecom sectors in India. We also have been deeply contributing to India's readiness in Cyber Security and Privacy, and conformance to Global Data Protection Regimes by our Industry Members. Privacy by Design is a concept which is very key to the Privacy charter of DSCI team and wish to assure you we will scale our efforts in Privacy Capability Building in the country on the same.

Iam grateful to the Chair and committee for incorporating several of my inputs into the Final Draft Bill.

Wish to place on record my special appreciation of Vidhi Legal Research team who worked tirelessly in Drafting the white paper and consultation exercise and helping draft the final versions.

My two colleagues Vinayak Godse, and Anand Krishnan contributed a lot to my research and contributions in the committee too.

While Iam very supportive of the overall Bill, I disagree with three provisions. Iam enclosing a note on the same. Would appreciate if it is placed as record in the Committee's Submission to Government.
However I wish to reassure you, that while I will continue to pursue advocating with Government as they undertake consultations in its enactment and enforcement, I stay committed to contributing deeply to help Government and our Industry members in getting ready to the new Data Protection Legislation and ensuring Privacy of Indians is protected. I also respect the chair and committee's endeavours in building a consensus, and the constraints in accepting all my inputs.

Thank You and assuring you of my support in implementation of the final Personal Data Protection Law.

Best Regards
Rama Vedashree

Note on THE PERSONAL DATA PROTECTION BILL, 2018

Rama Vedashree

Data Security Council of India (DSCI) and its Industry members have been advocating for a data privacy and protection law in the country for the last several years. We believe, the digital economy should primarily aim to benefit citizens, and the technology sector is fully supportive as the growth and proliferation of Information and Digital technologies is linked to citizen's feeling safe, secure and assured in the digital environment. DSCI since its inception has been working towards promoting data protection and is committed to equipping the industry through its capacity building initiatives to raise the threshold of privacy practices in India.

To ensure growth of the digital economy while keeping personal data of citizens secure and protected, it is important that as a country we take a balanced view that can meet the twin imperatives of safety and security of Indian data as well as enable the flow of global data into and from India.

The committee of experts under the chairmanship of Justice B.N. Srikrishna, has been working tirelessly for a year to achieve the goals laid down before us. The extensive Public Consultation and soliciting feedback from all stakeholders in India and across the world, and comprehensive review of inputs received has been a highlight of the Committee's deliberations. The framework proposed by the committee incorporates numerous provisions that lay emphasis on demonstration of accountability and re-establishing trust between entities and end consumers in the digital ecosystem.

But, with respect to certain provisions inscribed in the bill, I have a fundamental disagreement. This disagreement exists with respect to three provisions in particular.

First,the draft bill in its present form places restrictions on cross border flow of personal data. Under section 40(1) of the bill, this restriction translates into storing a copy of all personal data within India, while section 40 (2) completely restricts the cross-border flow of personal data for sensitive data categorised as critical personal data by the central government at its discretion, without inscribing guiding principles for this determination in the bill.

This approach is not only regressive but against the fundamental tenets of our liberal economy. Moreover, the inclusion of such restrictions in a bill that should focus primarily on empowering Indians with rights and remedies to uphold their right to privacy, seems out of place.

The committee report in chapter 6, projects localisation as tool for domestic market development. This narrative seems fuelled by unfounded apprehensionsand assumptions, rather than evidence and reasoning.

We as a country and Industry have been advocating the imperative of free flow of data and talent across borders. This is the foundation of the $167 billion IT-BPM industry represents and is India's largest foreign exchange earner ($110B in 2017-18). IT-BPM Service providers in India process financial, healthcare and other data of citizens and companies in the US, EU, and elsewhere in the world and have created employment for over 4 million people. Mandating localization may potentially become a trade barrier and the key markets for the industry

could mandate similar barriers on data flow to India, which could disrupt the IT-BPM industry. We are not` only a Global hub for corporations from more than 80countries, but also the destination for leading Global Corporations for R&D, Product Development and Analytics, Shared Services. We are also one of the largest growing technology start-up hub in the world, who from India are offering their innovative solutions and services to global geographies often leveraging global cloud platforms, thanks to the fundamental principle of Cross Border Data Flows and Internet economy.

Second, I disagree with the categorisation of financial data and password as sensitive personal data under section 3(35) of the bill. The guiding principles as mentioned in the report under chapter 3, for determining sensitivity are broad and can possibly be used to justify the inclusion of any type of data to this category of personal data. The concept of Sensitive Personal Data is primarily used for providing higher level protection to the data subject from instances of profiling, discrimination and infliction of harm that are identity driven. Neither financial data nor passwords fall into this category. It is also important to note, out of the 68 countries that presently have an overarching data protection regulation none have categorised financial data or passwords as sensitive personal data. These include countries from Asia Pacific, Europe and the Middle East.[1]

Third, the inclusion of criminal offences under chapter XIII of the draft bill is draconian. The Draft Bill and the Report,with steep fines and compensations advocate penalties which are sufficient to achieve the imperative of having deterrent penalties. The inclusion of criminal offences along with the fines and compensation is excessive and would impact the enforcement mechanism greatly. The enforcement tools should enable swift assessment and action to keep the process lean and approachable for the common man.

In addition to the above-mentioned points, the report under chapter 7 and the associated appendix, suggests sweeping amendments to the Aadhaar Act; these need a thorough review. I suggest a separate public consultation exercise by the government to examine these amendments.

I also request Government to publish the Bill, and the Report on MeitY's website, and conduct a round of Industryand stakeholder consultations before enacting the same.

[1]Please refer annexure 1.

Sensitive Personal Data Around the World As per July 2018

Source: Data Protection Laws of The World, DLA Piper **https://www.dlapiperdataprotection.com/index.htm**

No.	Country	Finanical Data	Passwords	Health Data	Genetic Data	Racial & Ethnic Origin	Religious Belief	Political Belief	Sex Life	Biometric Data
1	Angola	No	No	Yes	Yes	Yes	No	Yes	Yes	No
2	Argentina	No	No	Yes	No	Yes	Yes	Yes	Yes	No
3	Australia	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
4	Austria	No	No	No	No	Yes	Yes	Yes	Yes	No
5	Belgium	No	No	Yes	No	Yes	Yes	Yes	Yes	No
6	Bosnia and Herzegovina	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Bulgaria	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
8	Cape Verde	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
9	China	No	No	No	No	Yes	Yes	Yes	No	Yes
10	Costa Rica	No	No	No	No	Yes	Yes	Yes	Yes	No
11	Croatia	No	No	Yes	No	Yes	Yes	Yes	Yes	No
12	Cyprus	No	No	Yes	No	Yes	Yes	Yes	Yes	No
13	Czech Republic	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
14	Denmark	No	No	Yes	No	Yes	Yes	Yes	Yes	No
15	Estonia	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
16	Finland	No	No	Yes	No	Yes	Yes	Yes	Yes	No
17	France	No	No	Yes	No	Yes	Yes	Yes	Yes	No
18	Germany	No	No	Yes	No	Yes	Yes	Yes	Yes	No
19	Ghana	No	No	Yes	No	Yes	Yes	Yes	Yes	No
20	Gibraltar	No	No	Yes	No	Yes	Yes	No	Yes	No
21	Greece	No	No	Yes	No	Yes	Yes	Yes	Yes	No
22	Guernsey	No	No	Yes	No	Yes	Yes	Yes	Yes	No
23	Honduras	No	No	Yes	No	Yes	Yes	Yes	No	No

24	Hungary	No	No	Yes	No	Yes	Yes	Yes	Yes	No
25	Iceland	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
26	Ireland	No	No	Yes	No	Yes	Yes	Yes	Yes	No
27	Israel	Yes	No	Yes	No	No	Yes	Yes	Yes	No
28	Italy	No	No	Yes	No	Yes	Yes	Yes	Yes	No
29	Japan	No	No	Yes	No	Yes	No	No	No	No
30	Jersey	No	No	Yes	No	Yes	Yes	Yes	Yes	No
31	Latvia	No	No	Yes	No	Yes	Yes	Yes	Yes	No
32	Lesotho	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
33	Lithuania	No	No	No	No	Yes	Yes	Yes	Yes	No
34	Luxembourg	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
35	Macau	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
36	Macedonia	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
37	Madagascar	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
38	Malaysia	No	No	Yes	No	No	Yes	Yes	No	No
39	Malta	No	No	Yes	No	Yes	Yes	Yes	Yes	No
40	Mauritius	No	No	Yes	No	Yes	Yes	Yes	Yes	No
41	Mexico	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
42	Monaco*	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
43	Montenegro	No	No	Yes	No	Yes	Yes	Yes	Yes	No
44	Morocco	No	No	Yes	Yes	Yes	Yes	Yes	No	No
45	Netherlands	No	No	Yes	No	Yes	Yes	Yes	Yes	No
46	Nigeria	No	No	Yes	No	Yes	Yes	Yes	Yes	No
47	Norway	No	No	Yes	No	Yes	Yes	Yes	Yes	No
48	Philippines	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
49	Poland	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
50	Portugal	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No
51	Qatar	No	No	Yes	No	Yes	Yes	No	No	No
52	Romania	No	No	Yes	No	Yes	Yes	Yes	Yes	No
53	Russia	No	No	Yes	No	Yes	Yes	Yes	No	Yes
54	Seychelles	No	No	Yes	No	Yes	Yes	Yes	Yes	No

56	Slovak Republic	No	No	No	No	Yes	Yes	Yes	No	Yes
57	South Africa	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
58	South Korea	No	No	Yes	Yes	No	Yes*	Yes	No	No
59	Spain	No	No	Yes	No	Yes	Yes	Yes	Yes	No
60	Sweden	No	No	Yes	No	Yes	Yes	Yes	Yes	No
61	Switzerland	No	No	Yes	No	Yes	Yes	Yes	Yes	No
62	Taiwan	No	No	Yes	Yes	No	No	No	Yes	No
63	Trinidad and Tobago	No	No	Yes	No	Yes	Yes	Yes	Yes	No
64	Turkey	No	No	Yes	No	Yes	Yes	Yes	Yes	Yes
65	UAE - Dubai (DIFC)	No	No	Yes	No	Yes	Yes	Yes	Yes	No
66	Ukraine	No	No	Yes	No	Yes	Yes	Yes	Yes	No
67	United Kingdom	No	No	Yes	No	Yes	Yes	Yes	Yes	No
68	Uruguay	No	No	Yes	No	Yes	Yes	Yes	Yes	No

42	Monoco: Sensitive personal data is not expressly defined under the DPL but it is deemed to be:	
59	South Korea	The law uses the narrower term "creed" instead of Religious Beliefs

Vikash

From: Prof. Rishikesha T Krishnan [rishi@iimidr.ac.in]
Sent: Friday, July 27, 2018 3:19 PM
To: vikash
Subject: Fwd: Reservations regarding the Report of the Data Protection Committee

---------- Forwarded message ---------
From: Prof. Rishikesha T Krishnan <rishi@iimidr.ac.in>
Date: Fri, Jul 27, 2018, 3:11 PM
Subject: Reservations regarding the Report of the Data Protection Committee
To: B.N. Srikrishna <bnsrikrishna@gmail.com>
Cc: js gopal <js.gopal@meity.gov.in>

Dear Justice Srikrishna,
It has been a privilege for me to be a member of this Committee that has undertaken the most challenging task of envisioning a robust data protection framework for India. I thank you for providing an environment where free discussion of all issues was possible. I particularly laud your efforts to undertake extensive consultation with all stakeholders.

I am in broad agreement with the conclusions in the report and the accompanying draft bill.

However, I have reservations regarding the following which I would like to place on record. I would be grateful if these reservations could be recorded appropriately so that these are available to anyone who reads the report.

1. The requirement that every data fiduciary should store one live, serving copy of personal data in India is against the basic philosophy of the Internet and imposes additional costs on data fiduciaries without a proportional benefit in advancing the cause of data protection [Chapter 6 of the report].
2. The observations and recommendations regarding the Aadhaar Act are outside the scope of the committee's work.[Chapter 7 of the report].

Regards,

Rishikesha T. Krishnan