

*A Free and Fair Digital Economy:
Protecting Privacy, Empowering
Indians (Chapter 1)*

Justice B.N. Srikrishna, et al



A Free and Fair Digital Economy

Protecting Privacy, Empowering Indians

Committee of Experts under the Chairmanship of Justice B.N. Srikrishna (Members: A Sundararajan, AB Pandey, A Kumar, R Moona, S Gopalakrishnan, R Krishnan, G Rai, R Vedashree and A Sengupta)

Extracted below is Chapter 1 of the Report

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 Act² 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

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 destructive 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).

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 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 research¹² and Big Data generates more calibrated searches and allows quicker detection of crime.¹³ Large-scale data analytics allows machines to discern

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-healthcare-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).

patterns and constantly improves services in an endless virtual loop. The prospects of such data gathering and analysis to benefit citizens is immense.

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 data¹⁵ and mandate the implementation of a policy for dealing with such data.¹⁶ Further, various conditions such as consent requirement,¹⁷ lawful purpose,¹⁸

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.

purpose limitation,¹⁹ subsequent withdrawal of consent,²⁰ etc., have been imposed on the body corporate collecting such information.

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

¹⁹ Rules 5(4) and (5), SPD Rules.

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.

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. 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

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).

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).

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 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

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).

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.

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

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 Dymont (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.

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 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'être* 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.

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

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 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 cognizant 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.

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).

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 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.