Data Governance Network

November 2019

Working Paper 04

Fiduciary relationships as a means to protect privacy: *Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018*

Rishab Bailey and Trishee Goyal

National Institute of Public Finance and Policy

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The National Institute of Public Finance and Policy (NIPFP) is a centre for research in public economics and policies. Founded in 1976, the institute undertakes research, policy advocacy and capacity building in a number of areas, including technology policy. Our work in this space has involved providing research and policy support to government agencies and contributing to the creation and dissemination of public knowledge in this field. Our current topics of interest include privacy and surveillance reform; digital identity; Internet governance and rights, and regulation of emerging technologies. We also focus on research that lies at the intersection of technology policy, regulatory governance and competition policy.

Disclaimer and Terms of Use

The analysis in this paper is based on research by the National Institute of Public Finance and Policy. The views expressed in this paper are not that of the National Institute of Public Finance and Policy or IDFC Limited or any of its affiliates.

Cover page credit: Cactus Communications

Paper design: Cactus Communications

Suggested Citation

Bailey, R., Goyal, T. (2019). *Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018.* Data Governance Network Working Paper 04.

Supported by a grant from Omidyar Network

Abstract

In this paper we attempt to analyse the use of fiduciary law as a method to protect privacy of personal data in the draft Personal Data Protection Bill, 2018. We find that the PDP Bill does impose duties that are akin to traditional fiduciary obligations. However, the standard of loyalty expected of data fiduciaries is low. There is no requirement for the data fiduciary to act in the interests of or for the benefit of the data principal, merely a requirement to act in good faith. A higher standard could ensure greater rights protection. Instead the law chooses to empower the data protection authority to protect individuals from particularly significant risks.

Further, the fiduciary framing in the PDP Bill appears largely cosmetic. The use of the terms "data fiduciary" and "data principal" in itself adds little to the law. The law also does not implement any particularly novel rights or duties when compared to modern data protection laws (that do not use the fiduciary concept) such as the European General Data Protection Regulation.

Table of Contents

1. Introduction

Typically, a fiduciary relationship is one where a party holds a legal or ethical relationship of trust with another. The concept has been recognised in (common) law for hundreds of years - in the contexts of trusts (trustee / beneficiary), guardianship (guardian / ward), company law (director / company), agency law (principal / agent), etc. Recent literature has attempted to introduce the concept to the growing global discourse around privacy and data protection. Given the imbalances of power apparent in the context of ubiquitous data collection and use in today's digital economy, the concept appears intuitively attractive in that it establishes a duty of care on those using an individual's personal data, making it incumbent on them to act in the individual's interest. In the data protection context, this could mean for instance, the imposition of obligations concerning security of data, restrictions on sharing of data, or even a prohibition on practices such as profiling users, charging contextual prices or manipulating user behaviour.

Nevertheless, the concept has also been criticised, not least due to the apparent conflict the application of fiduciary duties may create with existing business models in the online economy that rely extensively on ubiquitous data collection.

In India, the public discourse around privacy and data protection has been steadily growing over the last few years. At around the same time as the declaration of the right to privacy as a fundamental right by the Supreme Court of India in the landmark (Puttaswamy v. Union of India 2017) case, the government constituted an expert committee under Justice (Retd.) Srikrishna in July 2017 (the "Committee" / the "JSK Committee") to study issues related to data protection in the country, suggest principles for data protection in India and propose a draft data protection bill.

The Justice Srikrishna Committee Report, which was submitted to the government in August 2018, introduces the concept of a fiduciary relationship into privacy jurisprudence in India, on the basis that the relationship between the "data principal" (i.e. individuals) and entities processing personal data (referred to as "data fiduciaries") is based on a "fundamental expectation of trust". The draft Personal Data Protection Bill, 2018,

(the draft "PDP Bill") accompanying the aforesaid Report attempts to operationalise the concept by establishing various rights of data principals and associated obligations on data fiduciaries.

In this paper we attempt to understand why and how the draft PDP Bill, attempts to utilise the concept of a "fiduciary relationship" to protect an individual's privacy rights. Specifically we attempt to examine:

- Are all data processing entities in fiduciary relationships with individuals?
- Are the obligations imposed by the PDP Bill similar to the duties expected of traditional fiduciaries?
- Does the use of fiduciary concept in the PDP Bill have any practical effect? Does it add anything novel to data protection frameworks that are typically based on notice-consent based models?

To answer these questions:

- *We first* provide an overview of the concept of a fiduciary relationship and try and understand why the law protects such relationships. Using examples from three commonly recognised fiduciary relationships - trustees-beneficiaries, company directors-companies, and doctors-patients, this section seeks to outline the general duties expected of a fiduciary in Indian law, and thereby provide a frame of reference to understand the use of the concept in the draft PDP Bill.
- *The second section of this paper* outlines how and why fiduciary relationships have been conceptualised in the privacy context in the US (i.e. the "information fiduciary" concept). We discuss the issue of whether all data processing relationships are fiduciary in nature, and the benefits and drawbacks of using the fiduciary concept to protect privacy rights. The section concludes with a brief overview of the use of the fiduciary concept in two recent (draft) privacy legislations in the US.
- We begin the *third section of the paper,* by exploring how the Justice Srikrishna Committee conceptualises the data principal-data fiduciary relationship. We examine the scope of the obligations imposed by the PDP Bill, with a view to

comparing these to the obligations imposed on traditional fiduciaries. Next, we briefly compare the obligations imposed under the PDP Bill to the European General Data Protection Regulation (GDPR). This helps in understanding whether the PDP Bill differs in any significant way from modern data protection frameworks. The section concludes by analysing the effects of the fiduciary framing in the PDP Bill, and speculates on the possible motives for the use of this concept.

2. What is a fiduciary relationship?

We begin this section by exploring why the law recognises and protects fiduciary relationships. We then examine what relationships are typically considered "fiduciary" in nature and the duties imposed in such relationships. In particular, we refer to the duties imposed by Indian law on company directors, trustees and doctors.[1]

2.1. Understanding the nature and purposes of a fiduciary relationship

There are numerous situations in our daily lives where we are required to place faith and trust in a second party in order to achieve an end that is recognised as being in the broader social interest. Think for instance of an agreement to buy goods. You are uncertain that the delivery will be of the goods ordered or that the quality of the goods will be as promised. In cases such as these, the law ensures you are protected through means such as contract or tort.

However, in certain relationships such legal protections may not suffice. This could occur, say, if the power imbalance between parties is relatively high thereby limiting their ability to contract in a free and fair manner. Contract law would merely forbid such contracts or enable restoration of status quo post breach. Social interest may

1 Note that a summary analysis of these three relationships is provided in Annexure I to this paper.

however require parties to enter into such relationships, without facing the possibility of adverse consequences.

Equity regards relationships which are characterised by a power differential or inequality between the parties, where one party is vulnerable to another and still required to impose trust and confidence in the other, as "fiduciary relationships" (Miller 2014). The law therefore seeks to ex-ante limit the possibility of the vulnerable party suffering harm.

The characteristic element of a fiduciary relationship is that the fiduciary serves as a substitute for the beneficiary (in meeting a particular end), and that the beneficiary is required to delegate power to the fiduciary in order to enable the meeting of that end (Frankel 1983) and (Miller 2014). This delegation of power however creates a vulnerability or a potential for abuse. This is the problem referred to as an "agency problem" - the fact that the agent may act in self interest.[2]

The law therefore steps in to temper the inequality in such relationships, where and to the extent other instruments of law cannot act (Frankel 1983) and (Rotman 2011). The purpose of recognising fiduciary relationships is therefore to enable interdependence while also protecting personal freedom, facilitating specialisation and enhancing productivity (Frankel 1983) and (Rotman 2011). In other words, the aim is to reduce agency costs and at the same time preserve the benefits of agency (Sitkoff 2014) and (Flannigan 2004).

To ilustrate, consider three commonly recognised fiduciary relationships - that of a trustee, a company director and a doctor.

- *Trustee - Beneficiary:* The concept of trusts developed to enable a landowner (settlor) to transfer property to a third party (trustee), to hold and deliver for a beneficiary, who was not normally qualified to hold title (say, due to being a minor) (Wynen 1949) and (Ames 1908). The trustee would be the legal owner of the property, but was bound in equity to hold it for the beneficiary.

2 An agency problem arises where one person, a principal, engages another, the agent "to undertake imperfectly observable discretionary actions that affect the welfare of the principal" (Sitkoff 2014).

Trusts therefore came to be recognised due to the imperfect ability of the both the settlor and the beneficiary to adequately monitor the behaviour of a trustee. Trustees, being the title holders and in physical possession of the property have the power to act in self-interest or otherwise abuse the faith shown in them. The vulnerability created by such relationships implies that the law needs to step in to protect the trust imposed by the settlor on the trustee (Leslie 2005).

- *Company director - Company:* A company, being an artificial creation, cannot act for itself. It functions through human agents - most importantly, its directors. Directors are officers, appointed by virtue of their expertise and professional skills to manage and run the affairs of the company. They therefore have significant power over the affairs and functioning of a company. Shareholders cannot be expected to practically or effectively supervise every action taken by a director on a daily basis (Radhabari Tea Co Pvt. Ltd. vs. Mridul Kumar Bhattacharjee and Ors. 2009) and (Nosworth 2016).

  In order to protect the interests of investors as well as that of the general public, the law recognises the relationship of a director with the company as a fiduciary relationship. This casts a series of duties and obligations of directors that aim to reduce the chances of abuse of a director's position (Douglas 1934).

- *Doctor - Patient:* Not all jurisdictions treat the doctor-patient relationship as a fiduciary relationship. Notably, English common law, while recognising the special nature of the relationship between a doctor and patient, does not specifically recognise it as being fiduciary in nature.[3]

  Jurisdictions such as the United States and Canada however, do recognise a doctor as a fiduciary. Patients entrust their bodies to the doctor leading to the creation of a power asymmetry between the two. There is also information asymmetry in the relationship due to the knowledge and experience that a doctor possesses.

3 See (Sidway v. Bethlem Royal Hospital Governors 1985). It has been suggested that common law has other suitable remedies to protect patients, and that deeming the relationship as fiduciary would entrench paternalism in English law thereby limiting the agency of patients (Bartlett 1997) and (Kennedy 1996).

A doctor can act unilaterally to the patient's detriment. Law therefore imposes various duties on doctors to ensure they do not abuse their power.[4]

Doctor-patient relationships have frequently been referred to as fiduciary by Indian courts (though this is mostly formulaic).[5] Indian law also imposes fiduciary duties on doctors through various statutes/regulations.

From the above, it is clear that generally speaking a fiduciary relationship exists where: (a) the beneficiary has a need to achieve certain ends that society considers valuable, (b) the fiduciary holds himself or herself out as able to achieve these ends, (c) the beneficiary has no or limited ability to monitor the fiduciary, and, (d) the fiduciary is in a position to unilaterally act to the detriment of the beneficiary. The law therefore steps in to ensure a more level playing field in the relationship by casting various duties on a fiduciary.

2.2. What relationships are "fiduciary"?

The law, first through tort and increasingly through statute, has recognised the concept of fiduciary relationships in an expanding number of contexts. But not all relationships that have an element of imbalance or vulnerability in them qualify as fiduciary.[6] The concept of a fiduciary relationship is applied "solely in regard to socially or economically important or necessary interactions of *high trust and confidence creating implicit dependancy and peculiar vulnerability*" (Rotman 2011).[7]

Whether a relationship is fiduciary or not is a matter of fact, determined by examining the degree of dependence and vulnerability brought about by the nature of the

4 See (Frankel 2011), (Moore v. Regents of University of California 1990), (Miller v. Kennedy 1987), (Norberg v. Wynrib 1979) and (McInerney v. MacDonald 1992).

5 See for example (Secretary General, Supreme Court of India v. Subhash Chandra Agarwal 2010) and (Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors. 2012).

6 For instance, car drivers are not recognised as being fiduciaries to pedestrians despite the imbalance in power and vulnerability in such relationships (Rotman 2011). Similarly, a restaurant is not a fiduciary to a customer despite the fact that the customer cannot exactly supervise the way the restaurant prepares his or her food (Rotman 2011).

7 The Supreme Court of India has used the term "fiduciary" to refer to a person *"having the duty to act for the benefit of another, showing good faith and candour, where such other person reposes trust and special confidence in the person owing or discharging the duty."* (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011).

relationship, the expectations of trust in the relationship and the social value of the relationship (Rotman 2011).[8]

While Indian courts often categorise a relationship as being fiduciary based on its re-semblance to commonly recognised fiduciary relationships, they have also laid down a series of tests to determine if a relationship can indeed be categorised as such.[9] Notably, in (Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. 2010), the court pointed out that a fiduciary relationship could be said to exist where confidence was reposed on one side and there was a resulting superiority and influence on the other. The vulnerable party must "expect to be protected or benefited by the action of the fiduciary" (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011).

However, one would require more than mere trust or vulnerability to qualify a relationship as fiduciary.[10]

In (Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. 2010), the Court went on to hold that a relationship can be considered to be fiduciary, if:

- The fiduciary has the scope for the exercise of some discretion or power;
- The fiduciary can unilaterally exercise that power or discretion so as to affect the beneficiary's legal or practical interests;
- The beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary holding the discretion or power;
- The fiduciary is obliged to protect the interests of the other party.

8 Per Black's Law Dictionary, quoted by the Supreme Court of India in (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011), fiduciary relationships can arise in the following situations: (a) when one person places trust in another, who as a result gains a position of dominance over the first, (b) when one person assumes control or responsibility over another, (c) when one person has a duty to act for or give advice to another on matters within the scope of the relationship, or (d) when there is a specific relationship that has traditionally been recognised as involving fiduciary duties.

9 Due to the difficulty in defining the specific nature of fiduciary relationships, courts around the world use the extension-by-association approach to gauge if a relationship is fiduciary or not. They compare the facts at hand to existing fiduciary relationships (usually trusts) to see if there are similarities. This has, per numerous commentators, led to less than satisfactory results and created a relatively incoherent body of jurisprudence (Rotman 2011), (Sitkoff 2014) and (Frankel 1983).

10 Here the court held that a authority conducting a public exam was not in a fiduciary relationship with the examiners engaged by it.

Indian courts have had numerous occassions to interpret the nature of fiduciary relationships (particularly in the context of information exchange).[11] Relying largely on the expectations of confidentiality with respect to the data exchange, the nature of power imbalance between the parties and the expectation of trust in the relationship, courts have *inter alia* recognised employees to be in a fiduciary relationship with employers qua information given to them in the course of their jobs,[12] examiners in public exams to be in fiduciary positions qua the examining board,[13] a bank towards a client,[14] and officers in the JAG branch of the armed forces to be in fiduciary relationships qua information recieved in the course of their duties.[15] In a recent case, the High Court of Kerala has held that an individual's banking related information - being personal/private in nature - was held by the bank in its fiduciary capacity. The bank would therefore have to maintain the secrecy of such information, unless disclosure was required by law.[16] In all these cases, the primary duty of the fiduciary was to ensure the confidentiality of the relevant information - whether personal data or not. This duty is independant of any specific contract between the parties.

On the other hand, Courts have held that board examination authorities are not fiduciaries qua students,[17] the central bank is not a fiduciary qua other banks,[18] the

11 Notably, in the context of (a) Section 88 of the Trusts Act which *inter alia* prohibits profiting at the expense of the beneficiary in any relationship of a fiduciary character, and (b) Section 8 of the RTI Act which prohibits disclosure of information by a public authority, when recieved in a fiduciary capacity.

12 (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011) and (M. Kanniyappan vs. The Presiding Officer, Labour Court and Ors. 2011).

13 (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011), (P Kishore Kumar and Ors. v. The State of Andhra Pradesh and Ors. 2016) and (The Institute of Chartered Accountants of India v. Shaunak H Satya and Ors. 2011).

14 In respect of certain financial services the bank was providing for the beneficiary by purchasing financial instruments on his behalf (Canbank Financial Services Ltd. v. Custodian and Ors. 2004).

15 (Union of India and Ors. v. VK Shad and Ors. 2012).

16 Here, the court was examining the validity of notifications issued by state owned petroleum suppliers, who had asked distributors to provide bank account details and income tax information to enable them to check benami holdings. It was argued on behalf of the suppliers that banking information was already available with banks, and therefore no right to privacy should apply to such data. Holding that the right to privacy is not lost as a result of confidential information being parted with by a customer to a bank, the court observed that the relationship between a bank and its client was fiduciary in nature. The court ultimately found that no law authorised the suppliers to demand personal information, and therefore struck down the relevant notifications as violating the fundamental right to privacy (Raju Sebastian and Ors. v. Union of India and Ors. 2019).

17 The relationship betwen the parties being that of a service provider and consumer (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011) and (Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors. 2012).

18 There being no legal duty to maximise the benefit of banks or a relationship of trust between the central bank and other banks (Reserve Bank of India v. Jayantilal N Mistry 2015).

chief justice is not a fiduciary qua puisne judges of the supreme court,[19] banks are not fiduciary's towards their clients,[20] while tax assessees are not fiduciaries of the tax department.[21]

Overall, Indian courts appear to have taken pragmatic positions based largely on the facts before them and the nature of competing interests at hand. Interestingly, Indian courts have also recognised that relationships can have both fiduciary and non-fiduciary aspects.[22] The standard of care expected in fiduciary relationships would apply to the fiduciary portion of the relationship.

2.3. Fiduciary duties

The primary method of addressing the agency problem in fiduciary relationships is by placing a series of onerous, principle based duties on the more powerful party. Equity attempts to establish a relationship between parties that restricts opportunities to breach faith, rather than merely contemplating restitution of status quo. It therefore enforces a higher moral standard than other forms of legal remedy (Ames 1908).[23] The purpose of implementing such a standard is to provide a measure of control to the beneficiary, ensure its interests are properly protected, and enable a court to, in effect, retrospectively read in terms that parties would have entered into had all the facts (including any resulting harms) been known at the time of contracting (Sitkoff 2014).

19 The information provided by judges to the chief justice is not provided in trust. The relationship between the parties is not hierarchical and there is no element of control or dominance (Secretary General, Supreme Court of India v. Subhash Chandra Agarwal 2010).

20 Here the bank had retained proceeds from the auction of goods imported by a trader on account of a letter of credit supplied by them. It was held that such an amount was not held in a fiduciary capacity (Krishna Gopal Kakani v. Bank of Baroda 2001).

21 Information is provided to the authority under statute and not through choice (Naresh Trehan vs. Rakesh Kumar Gupta 2014), (Shri Rakesh Kumar Gupta vs. The Central Public Information Officer and The Appellate Authority, Director of Income Tax (Intelligence) 2011) and (Reserve Bank of India v. Jayantilal N Mistry 2015).

22 "Fiduciary relationships may be confined to a particular act or action and need not manifest itself in entirety in the interaction or relationship between the two parties." (Union of India v. Central Information Commission 2009). Also see (Canbank Financial Services Ltd. v. Custodian and Ors. 2004).

23 Fiduciary relationships establish an altruistic relation between the parties - the fiduciary is expected to place his or her interests subservient to that of the beneficiary. This is different to say contract law, which is underpinned by a morality that seeks to preserve the self-interest of both parties (Frankel 1983). Also see (Union of India v. Central Information Commission 2009). Notably, Indian contract law does not expressly recognise duties of good faith - parties are expected to act in self-interest.

The two most important duties in a fiduciary relationship are the duty of loyalty and the duty of care (Frankel 2011).

- **Duty of loyalty and care:** The duty of loyalty implies the fiduciary's responsibility not to misappropriate/misuse the property, opportunity or information of the beneficiary and not to undertake any action, or put themselves in a position that may be seen as conflicting with the interests of the beneficiary.[24] The duty of care implies that the fiduciary must act "in good faith" towards the beneficiary i.e. must act in a bona fide and fair manner in accordance with generally accepted practice.

  There is no single standard of loyalty across different types of fiduciary relationships though the beneficiary's interests must always be placed before that of the fiduciary. Standards of loyalty include for example, requirements to act in the beneficiary's "best interests" or "sole interests", to act "without causing detriment", to act to the "manifest advantage" of the beneficiary, to act to the "benefit of" the beneficiary, etc.[25]

  Though the fiduciary may obtain the beneficiary's consent to act in conflict, this, if permitted will usually be subject to defined safeguards such as requirements of substantive and specific information disclosure (Sitkoff 2014).[26]

  To illustrate, we examine the duties of loyalty and care cast by Indian law on trustees, directors, and doctors.

24 The duty of loyalty can be interpreted to mean different obligations in different contexts such as duties not to compete with the beneficiary for business opportunities, to always act so as to maximise profit to the beneficiary, not to profit at the expense of the beneficiary, etc.

25 Refer (Sitkoff 2014), (Langbein 2005) and (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011). Also see the analysis of the duty of loyalty in Indian law contained in Annexure - I to this paper. Standards of loyalty are based on the specific nature of vulnerability in the relationship and the reasonable expectations of parties and may therefore differ from relationship to relationship. For instance, trust law is said to cast more onerous obligations on fiduciaries than company law (Rotman 2011).

26 There is no certainty in academic discourse about whether fiduciary relationships impose freely waivable default rules or whether they contain a non-waivable core. It is argued that certain essential elements of a fiduciary relationship such as the duty of loyalty and care cannot be eliminated in entirety. (Leslie 2005) for instance, argues that no court would uphold a trust provision seeking to elminate the trustee's duty of loyalty in entirety. Were fiduciary arrangements completely optional, they would be nothing more than mere contracts. However, fiduciary relationships exist as the information asymmetry and consequent vulnerabilities in the relationship imply that even including specific contractual terms may not adequately help the beneficiary or settlor make a judgment as to value maximisation. This position appears to find acceptance in obiter of the Delhi High Court which has observed in (Union of India v. Central Information Commission 2009) that fiduciary relationships "may not be readily tailored and modified to suit the parties."

– The context of *trusts,* the most essential duty is that of the trustee acting in good faith, and in the interests of the beneficiary (Clarry 2014). The requirement of good faith and loyalty is so high that trustees are not even entitled to recieve payments for their services - trusteeship is not an office of profit.[27] Multiple provisions of the Indian Trusts Act, 1882 (hereinafter the "Trusts Act") such as Sections 52, 53, and 88, contain prohibitions on self-dealing[28] and requirements of fair dealing.[29] To illustrate, under Section 52, Trusts Act, a trustee cannot, directly or indirectly, purchase trust property intended for sale, on his or her own account or as an agent for a third party. The law does not go into the question of whether the transaction is beneficial or not but just assumes fraud in such cases (Swaminatha Aiyar v. Jumbukeswaraswami 1930) and (Morse v Royal 1806).[30] Similarly, Section 53 permits a trustee to purchase the interest of a beneficiary only subsequent to court permission, which will only be given when the court is satisfied that the transaction is 'manifestly to the advantage' of the beneficiary. Section 88 prohibits the trustee (or any other party in a fiduciary relationship) from using their fiduciary position to gain a pecuniary advantage or placing themselves in a situation where they may profit from a conflict of interest. Any such profit made, is held for the beneficiary.

– As far as *company directors* are concerned, this duty is recognised in numerous provisions of the Companies Act, 2013, (hereinafter the "Companies Act") notably in Sections 166(2), (4) and (5).[31] The statute is clear in not

27 Section 50 of the Trusts Act recognises that a trustee cannot expect payment for services rendered by default i.e. he or she is entitled to renumeration only when the same is specifically granted in the trust instrument, by order of court or by contract with the beneficiary. Trusts therefore differ from certain other fiduciary relationships where remuneration is accepted as part of the service.

28 Under the self-dealing rule, the trustee is not allowed to sell trust property to himself. In case he sells to himself, the transaction is rendered voidable at the option of the beneficiary, regardless of how fair the transaction is.

29 Under the fair-dealing rule, the transaction can be set aside by the beneficiary unless the trustee can show that he has taken no advantage of his position and has made full and material disclosures to the beneficiary, and that the transaction is fair and honest.

30 In order to prevent any possibility of self-dealing, the law presumes invalidity of certain acts, not because there is fraud, but just because of the possibility that there may be fraud (Langbein 2005).

31 Sections 166(2) and (4) are said to convert longstanding common law duties into statutory ones by requiring directors to act in "good faith" to promote the objects of the company and by prohibiting the director from acting in situations where he or she may have a conflict of interest with the company (Narayandas Shreeram Somani v. The Sangli Bank Ltd. 1965). Section 166(5), Companies Act specifies that a director should not achieve or attempt to achieve any undue gain or advantage either to himself or to certain related parties and if found doing so, is liable to account for the same.

just requiring directors to avoid a direct conflict of interest - but also stops them from entering situations where there is a mere possibility of such a conflict. Director's may however engage in such transactions, subsequent to adequate and specific information being provided to the company, and consent being obtained.[32]

As an example, take the case of a director's powers to issue further capital. Courts have uniformly held that this power, by virtue of being exercised in a fiduciary relationship, can only be used in the interests of the company itself.[33] The power to issues shares cannot be used by the director to directly seek to enrich himself at the cost of the company. In situations where the director profits as a result of the exercise of powers, this would only be valid if this benefit is incidental and not the main motive of the further issue.[34]

The exercise of such powers must be bona fide[35] and must be done with a proper motive i.e. for reasons that place the beneficiary's interests first[36]

– In a *doctor-patient relationship,* doctors are typically required to place the patient's considerations over others, including their own.[37] To this end, the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (hereinafter the "IMC Regulations") contain numerous provisions that regulate a doctor's possible conflicts of interest - notably in the cases of providing excessive services, prescribing treatments in which

32 As an aside, Section 197 of Companies Act also limits the possibilities of a director taking advantage of a company by capping the maximum managerial remuneration. Any sums received by the director above the prescribed limits are to be held in trust for the company.

33 Refer (Nanalal Zaver and Ors. v. Bombay Life Assurance Co. Ltd. and Ors. 1950), (Needle Industries (India) Ltd. and Ors. v. Needle Industries Newey (India) Holding Ltd. and Ors. 1981) and (Ram Parshotam Mittal and Ors. v. Hotel Queen Road Pvt. Ltd. and Ors. 2019).

34 Refer (Ram Parshotam Mittal and Ors. v. Hotel Queen Road Pvt. Ltd. and Ors. 2019) and (Needle Industries (India) Ltd. and Ors. v. Needle Industries Newey (India) Holding Ltd. and Ors. 1981).

35 There must be a genuine need for the company to undertake the exercise of issuing shares (though this may not need to be limited to the raising of capital).

36 That is, it should not be done to maintain the director's own standing in the company or to limit the powers of specific shareholders, etc. (Dale and Carrington Invt. (P) Ltd. and Ors. v. P. K. Prathapan and Ors. 2005).

37 Refer for instance to the modern Hippocratic oath which states that "The health and well being of my patient will be my first consideration" and the original version which provides "…I will do no harm or injustice to them… Into whatever homes I go, I will enter them for the benefit of the sick, avoiding any voluntary act of impropriety or corruption, including the seduction of women or men, whether they are free men or slaves" (Parsa-Parsi 2017) and (North 2002).

the doctor has an interest, referring patients for a fee, receving benefits from pharmaceutical companies, etc.[38]

Though not per se barred from indulging in all practices that may enrich themselves, doctors must provide sufficient information about any conflicting interests to the patient.

- **Standard of care:** Fiduciaries are required to maintain a high standard of care in carrying out their activities. Generally they are required to act in a reasonable or prudent manner informed by expected practices or industry norms. The standard of care is objective in that it is that of a reasonable person in possession of the relevant qualifications and skills (Sitkoff 2014).

  A similar standard can be seen in the context of the Indian law pertaining to directors, trustees and doctors (refer Annexure - I).

Fiduciary law butresses the aforementioned basic duties with a range of subsidiary duties that enable the agency problem to be resolved in the particular circumstances of the relationship at hand. These duties are primarily designed to reduce the information asymmetry problems inherent in fiduciary relationships, and reduce the fiduciary's opportunities to act in self-interest.

For instance Indian company law, trust law and medical law all:

- *Contain strict requirements of information disclosure:* To illustrate, sections 19 and 57 of the Trusts Act require the trustee to keep clear and accurate accounts of the trust property and furnish full and accurate information to the beneficiary as regards the amount and state of trust property, respectively. Similarly, sections 170, 184, 189, 129, and 102 of the Companies Act requires a range of disclosures to be made by directors to the company pertaining to their identities, interests held by them and possible conflicts, the status of the company, etc. The Indian

38 For example, Regulation 1.1.2 of the IMC Regulations recognises that financial gain should be a subordinate interest to the patient's well being. Doctors are also beholden to remember that patients depend on them. Doctors having an incapacity "detrimental to the patient" or which can affect performance of duties are not permitted to practice.

Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (IMC Regulations) also require disclosures to be made by doctors to their patients "in their best interests". Patients must be provided information on the nature and procedure of treatment (purpose, benefits, effects), alternatives, substantial risks and possible adverse consequences of refusing treatment (Dr. Prabha Manchanda 2008). Doctors are also obliged to provide the patient with his or her own medical records, within a period of 72 hours from a request (Sameer Kumar v. State of Uttar Pradesh 2014).

- *Limit the ability of the fiduciary to act outside the bounds of what is expected by the beneficiary:* For example, section 11 of the Trusts Act requires trustees to fulfill the purposes of the trust, and to obey the instructions of its settlor, except as modified by consent of the beneficiaries (who must be competent to contract). Similarly, section 166(1) of the Companies Act requires directors of a company to act within the limits of the authority conferred on them by the articles of the company.

Importantly, fiduciary law confers an independent cause of action for the beneficary against the fiduciary, irrespective of the existence of a contract between the parties (Frankel 1983).[39] The cause of action can arise from mere breach of the duties imposed. Further, the damages available for breach of fiduciary duties tend to be on the higher side. This is so as to deter fiduciaries from abusing their positions (Sitkoff 2014).[40] The above is also, generally speaking, in accord with the obligations imposed by Indian law pertaining to doctor-patients, directors-companies, and trustee-beneficiary relationships. A more detailed analysis of these relationships is provided in Annexure - I to this paper.

39 The burden of compliance is on the party holding power in the relationship (Rotman 2011).

40 A fiduciary's failure to follow norms of behaviour creates uncertainty, thereby increasing transaction costs for the vulnerable party in the relationship. Fiduciary law attempts to stigmatise opportunist behaviour by limiting the abilities of fiduciaries "to stretch the boundaries of acceptable conduct" (Leslie 2005).

3. Information fiduciaries: What are they and why use the fiduciary concept to protect privacy?

The concept of treating digital service providers as fiduciaries has been largely associated with Professor Jack Balkin.[41] He proposes using a fiduciary based framework for protecting individuals in their interactions with social media companies and other entities in the digital economy that process personal data on a large scale.[42] This framework would see a variety of fiduciary-like obligations imposed on service providers, under a "Digital Millenium Privacy Act".[43]

Balkin's thesis, though influential and widely accepted, is not without its critics though these are few and far between.[44]

In this section of the paper we examine the arguments made for and against the 'information fiduciary' concept. We try and understand why the information fiduciary concept has been used in the data protection context, whether digital service providers are fiduciaries, and the possible effects of treating them as such.[45] We conclude with an overview of how two recent American legislations attempt to operationalise the concept.

41 Professor Kenneth Laudon was the first to seek to apply fiduciary principles in the context of the digital economy. Laudon's work "Markets and Privacy" was one of the first to propose recognition of an individual's property rights in their personal data. While not specifically theorising a way to "protect" users from privacy harms, he suggested creating a national information market where individuals can control the sale of their data and recieve fair compensation for its uses. Laudon conceptualises "information fiduciaries" as entities who would participate in the information market as delegates for individuals - who would not normally have the time or interest to participate in the market directly. These entities would act as agents by accepting deposits of information (much like banks accept depositor money) and then seeking to monetise that information in exchange for a fee or percentage of returns (Laudon 1993).

42 Balkin has written about the concept in a series of blogs and papers beginning in around 2014 (J. Balkin 2014).

43 The law would provide safe harbour to service providers, from privacy claims brought under American state laws and tort, in exchange for voluntary compliance with the obligations imposed thereunder. This forms part of a "grand bargain" under which companies that elect to be information fiduciaries would be able to avoid liabilities under evolving privacy law (J. M. Balkin and Zittrain 2016).

44 Lina Khan and David Pozen provide the only significant critique of the concept in their paper "A skeptical view of information fiduciaries" a draft of which was released in early 2019. Others such as (Bambauer 2016) also criticise certain parts of Balkin's thesis, though primarily concerning first amendment issues.

45 This exercise is particularly relevant given that the Committee specifically relies on Professor Jack Balkin's 2016 paper to develop the concept of a fiduciary relationship in the Indian data protection context. (J. M. Balkin 2016).

3.1. Why use the data fiduciary concept?

Balkin's thesis draws from four main motivations:

- **First Amendment issues:** The US Constitution privileges speech over privacy rights (J. M. Balkin 2016). This implies that any comprehensive data protection framework is likely to face constitutional challenges in view of the limitations it will place on free spread of information.

  Balkin therefore proposes the information fiduciary concept as a way to justify imposing data protection related obligations on large service providers. By *inter alia* seeking to tailor regulations to specific classes of relationship (rather than classes of speech), Balkin suggests that it is constitutionally permissible for the government to impose restrictions on processing of personal data exchanged in private contexts (J. M. Balkin 2016).

- **Notice and consent based models fail to sufficiently protect users:** Balkin points to how the US privacy framework (when it comes to an individual's rights against the private sector) is severely lacking as users are unable to properly assess the risks of giving consent (J. M. Balkin 2018).[46] He therefore advocates using the fiduciary approach as it would allow information fiduciaries to be held to reasonable and ethical standards of behaviour, based on expectations of users, even without the existence of specific representations (J. M. Balkin 2016).[47] The concept would preserve the autonomy of parties (as it would permit users the ability to decide what relationships they want to engage in) and addresses some of the critical concerns of a notice-consent based system including by putting the onus on the fiduciary to demonstrate specific and meaningful consent was appropriately secured (J. M. Balkin 2016).

- **Proportionate and technology neutral approach:** Balkin points to how the information fiduciary concept, could enable the imposition of a sliding scale of

46 Also refer to (Bailey, Parsheera, Rahman, and Sane 2018) for a summary of some of the problems of notice and consent regimes.

47 Balkin notes that the fiduciary approach does not rest entirely on consent. It requires fiduciaries to act in good faith or in the interests of the beneficiary. This goes beyond the normal contract law framework under which parties are free to pursue individual interest.

obligations as it is based on the nature of relationship at hand and the objective expectations of users. This enables tailoring the data protection framework to different contexts based on reasonableness of the specific practice at hand (J. M. Balkin 2016). This makes the system particularly attractive due to the contextual nature of privacy rights. The concept sets out general expectations and duties without being overly prescriptive. Business practices that violate commonly held and reasonable expectations of users will be barred.

The concept is also technology neutral in its approach and can apply to a wide range of the biggest data processing industries - such as social media companies, email service providers, etc. (J. Balkin 2014).

- **Vulnerability in relationship of users and service providers:** The final, and most vital reason for use of the fiduciary concept is the conviction that relationships between users and service providers in the digital ecosystem are underscored by a power imbalance.

  Users are required to provide their (often sensitive) data to online services (in order to use or access these services), who are strangers. This places users in a position where their trust may be abused.

  (J. M. Balkin 2016) points specifically to three types of asymmetries that create such an imbalance:

  – *Asymmetry of information:* This stems from the fact that user's have very little information about online service providers and what they can do with the information they have collected. However, online service providers can easily monitor what user's do and collect data about them. The sensitive information that the service provider collects may be used to the user's disadvantage.

  – *Assymetry of power:* User's are in a position of relative dependence on digital service providers, especially as those services are important to them. Further, the quality of some of these services is dependent on the service providers utilising the users' personal information.

– *Assymetry in transparency:* Users are transparent to online service providers, but the latter's operations are not transparent to the former. Online service providers know that user's know that they hold valuable data and accordingly make statements aimed at reassuring and gaining their trust i.e. they hold themselves out as trustworthy organisations. Service providers also keep their operations secret for competitive and security reasons. Therefore, despite the fact they cannot be fully transparent, users are required to place their trust in them.

Balkin therefore believes that the law can and should treat certain categories of data service providers as fiduciaries, based on the nature of the relationship at hand and the reasonable expectations of users. This would allow the law to impose duties of care and loyalty on service providers, which would permit for data protection while at the same time maintaining user autonomy.

3.2. Are (all) digital service providers information fiduciaries?

Today's digital ecosystem sees a wide variety of actors who in the general course of their activities process personal data. This can range from individuals using their smartphones to record other individuals, to big corporations collecting large quantities of personal data from public and private locations. It is therefore important to understand if the information fiduciary concept can adequately cover all relevant data processing entities within its scope.

Balkin does not believe there is a need for all entities processing personal data to be considered information fiduciaries (J. M. Balkin 2016). He clarifies that any such classification should depend on the nature of the asymmetries at hand. Balkin argues that it is not the mere exchange of information that creates the fiduciary relationship. The fiduciary character of the relationship is based on the *nature* of the relationship between the parties, the *reasonableness of trust* placed by the user on the service provider based on existing norms of behaviour and existing industrial practice, and the *importance of preventing self-dealing or harm* to the user (J. M. Balkin 2016). Therefore only those

relationships where there is a *special* vulnerability created, or where service providers look to specifically *induce* trust would be covered by the scope of the concept.[48] (Dobkin 2018), who expands Balkin's thesis, specifically exclude companies such as data brokers from the concept altogether (as their business models go completely against the concept of fiduciary relationships).

The theory of information fiduciaries is therefore fairly narrowly conceptualised. It only attempts to address the harmful practices committed by a limited set of actors in the digital ecosystem (J. M. Balkin 2016). By doing so the concept avoids first amendment related restrictions and protects the quality of public debate.[49]

The narrowness of the concept however detracts from its utility as a general data protection framework. As pointed out by (Bambauer 2016), many digital service providers do not seek to endanger a relationship of trust with their users and they would therefore fall outside the scope of the information fiduciary concept. Further, personal data, even when provided in prima facie personal contexts can be misused (that too against the expectations of users) particularly in the digital environment.[50]

In the Indian context, free speech issues are less relevant than in the US. Nonetheless, courts have consistently held that fiduciary relationships would only exist where there is a significant vulnerability in the relationship between the parties, and where there is a duty for one party to act for the benefit of the other.[51] As noted previously,

48 Balkin argues that large digital companies look to "induce" user's to trust in their services (so that users will continue to use their services), and that users believe that their data will not be used maliciously or against their interests. This is said to be similar to the expectations in a doctor-patient or lawyer-client relationship, which are typically recognised as being fiduciary (J. M. Balkin 2016), and (J. Balkin 2014).

49 (Bambauer 2016) points out that enhancing the scope of the concept to extend to any relationship of information exchange where there is even the slightest imbalance in trust and vulnerability or where one party was relatively uninformed or dependant, would bring within its scope many relationships such as that between spouses, friends, co-workers, and so on. The need to place fiduciary obligations in all these relationships would unduly restrict information exchange in society (Bambauer 2016).

50 Data protection rights in advanced regimes (such as under the European Union's General Data Protection Regulation (GDPR)) recognise privacy rights in far greater contexts than that proposed by Balkin, and apparently without significantly adverse effects on the quality of public discourse (though European standards of speech protections are significantly different to that in the US, being more comparable to that in India). See for instance, the case of (Bodil Lindqvist v. Aklagarkammaren i Jonkoping 2003), where it was held that the publication of a list of friends and information pertaining to them on a blog maintained by an individual, would fall within the scope of the European data protection framework (i.e. it would not be covered by the exception for personal use).

51 See (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011) and (Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. 2010).

relationships involving information exchange between a service provider and customer have been held to not constitute fiduciary relationships in some contexts.[52] Every day relationships of information exchange that create only a limited vulnerability between the parties, whether in the online world or not, would therefore be excluded from the information fiduciary concept.

On the other hand, Indian courts have allowed separation of fiduciary parts of a relationship from other parts thereof. This could imply that a relationship not normally fiduciary in nature, could possibly be considered as such, only with respect to the transfer of information and the expectation of trust created thereby. Indian courts have also largely relied on (a) the fact that information is confidential or private in nature, (b) that there is an expectation that it will be maintained as such, in deciding whether it is protected under the fiduciary concept.

While the concept may be narrow in so far as its coverage of relevant entities is concerned, it does permit itself to expansion both in the scope of duties that could be made applicable to entities or indeed the scope of the data that forms the basis for the relationship. The fiduciary concept does not have to be restricted merely to protect "personal data" (i.e. data that relates to or identifies an individual) but can cover all types of data that are exchanged in a unequal relationship, with an attendant expectation of confidentiality (i.e. the data should not be publicly known information). The concept could therefore be seen as enabling a greater degree of protection than under frameworks such as the GDPR (which restrict themselves to protecting personal data), by also casting obligations on usage of non-personal data gleaned from a user, as well as non-personal data derived from personal data of a user (as long as the data is given with an expectation of confidentiality, etc).[53]

52 Refer (Reserve Bank of India v. Jayantilal N Mistry 2015), (Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors. 2012) and (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. 2011). Though in certain other contexts, such as that of a banker and its customer, such relationships have been held to be fiduciary in sofar as the information given by a customer to the bank is concerned (Raju Sebastian and Ors. v. Union of India and Ors. 2019).

53 Note that in many of the Indian cases discussed previously, confidentiality restrictions are imposed on *non-personal data* using the fiduciary concept.

In addition to addressing the breadth of the concept, one may argue that *any* service provider-user relationship is not fiduciary in nature. We examine the grounds for this argument below:

- **Conflict of interest:** The fiduciary concept requires the beneficiary's interests to be placed before that of the fiduciary. The law requires altruistic behaviour of the fiduciary as opposed to acting in self interest. (Khan and Pozen 2019) believe that this is not possible in the digital ecoystem given the in-vogue business models that rely on bulk data collection and targetted advertising. Further, the change in business model required for such a re-alignment of interests would vitiate from company law obligations that place shareholder interests before that of any other stakeholder.

  However, fiduciary law does recognise multiple standards of the duty of loyalty - based on the information asymmetry at hand, the nature of the relationship, the ability of the beneficiary to understand the risks involved and so on.[54] Deviation from the high standard of care is permitted subject to appropriate safeguards (for instance, informed consent subsequent to disclosures or court approval). Illustratively, company law implements a slightly lower standard as far as conflict of interest is concerned than trusts (Langbein 2005). Directors are to adhere to standards of fair dealing (implying genuineness and bona fide behaviour) rather than acting with the sole obligation of protecting the beneficiary.[55]

  It does not therefore appear inconceivable for the information fiduciary concept to be made workable. Such a standard *could indeed force service providers to change some of their business models,* with or without a complete bar on targetted advertising.[56]

54 Fiduciary duties being equitable in nature, do not in and of themselves require a specific standard of care to be followed "inexorably" in all situations (Industrial Development Consultants v. Cooley 1972).

55 Taking a strict view, a fiduciary can be expected to "maximise the benefit" to the beneficiary in a relationship of trust (Reserve Bank of India v. Jayantilal N Mistry 2015). Fiduciary relationships such as trusts are also seen as not-for-profit relationships. Company directors however are not altogether prohibited from making profits. They are largely just required to disclose their competing and other interests.

56 Higher standards of care could be made applicable if based on the facts at hand - say caused by the volume or type of information processed, the existence of a monopoly of the service provider, etc. - greater vulnerabilities were to be found in any particular relationship. In any event, the question of whether targetted advertising is against social interest or not, is still open to debate. Delivery of targetted ads could for instance, be justified from the user's perspective as an extention of the right to recieve information. Personal data can also be used to deliver customised services and the like (which could be seen as being in the interests of the user given the efficiencies involved).

Further, there is no reason why statute cannot place the duties of a service provider above those owed towards shareholders. Many jurisdictions, as in the case of the UK and India, cast broad fiduciary duties on the directors of companies (including by recognising their duties towards society generally), meaning that this criticism is less likely to be a deal-breaker outside jurisdictions such as Delaware.[57]

- **No personalised or expert services:** Khan and Pozen argue that a traditional fiduciary offers professional skills and expertise, which a digital service provider doesn't. They rely on generic algorithms to service users. Even if they could be considered to be providing some level of specialised service, say when undertaking personalised content curation, they do not bring any expertise to bear on behalf of their users (Khan and Pozen 2019). In addition, one may also point to the absence of any "delegation" by a user to a service provider. Often the ends the service provider is working towards have nothing to do with the user, who merely provides raw material in the form of personal data.

  Companies do indeed service many users with the same algorithms. Nevertheless, the effects of this are unique/individual and real. Just as doctors may have set ways of interacting with and eliciting information from patients before prescribing a choice of treatment based on the answers of the patient, algorithms input specific personal data based sets and produce personalised results for users of digital services.[58] Further, not all companies use the same algorithms or algorithms that function in the same fashion, even if leading to superficially similar results (for instance, different search engines will recommend content in different ways, even if acting on the same sets of user data). A certain level of expertise could indeed be said to be present in the relationship.

  Further, not all relationships deemed fiduciary in nature always require completely "personal" relationships. For instance, public trusts can be considered fiduciary

57 (Khan and Pozen 2019) recognise that this is a possible solution to the matter - that it could be argued that by placing user interests first, companies are acting in their long-term interest by preserving the relationship with users, enhancing their reputation and brand value, etc. They however they reject the possibility of such a view being taken in Delaware company law, where many large internet based companies are incorporated.

58 The increasing use of algorithm based applications even in medicine further bears this out.

relationships as can government-citizen relations.[59] As described previously, Indian courts have also recognised relationships such as that between examiners and examining boards (which function based on strictly defined rules for grading exams), and employers-employees as fiduciary in nature.

- **Differences in the nature of information asymmetry:** (Khan and Pozen 2019) point to how the nature of asymmetries present in a traditional fiduciary relationship are qualitatively different to that in a user-service provider relationship. Clients in traditional fiduciary relationships can understand the core principles of the relationship and therefore exercise some control over the fiduciary, which is not possible in the digital ecosystem.

  This argument relies on a qualitative assessment and is therefore not particularly convincing. For instance, European authorities point to how implementation of the GDPR has lead to a significant increase in user awareness of privacy rights.[60]

  There are undoubtedly reasons to be concerned about whether the information fiduciary concept can adequately deal with the information asymmetries in the digital ecosystem. However, the fiduciary concept is to a large extent directed at improving standards of consent. Fiduciaries will not be able to "trick" users, act dishonestly or seek to take advantage of them. The onus will be on the service provider to show that the user was provided sufficient information so as to be able to consent to a particular practice. It will also be possible for courts to deem a practice so unreasonable or against social norms, that a user would never consent to this even if informed thereof.

- **Created vulnerability:** (Khan and Pozen 2019) note that in a traditional fiduciary relationship, information is provided to the fiduciary to enable him or her to carry out his functions. Providing personal data is however not a functional prerequisite for accessing digital services, being a voluntary choice of the companies

59 See for example (Tsosie 2003), (Ezra 1989), (Hurley 2002), (Davis 2014). The Indian Supreme Court has also observed that the states relations with citizens is akin to a fiduciary relationship (Kapila Hingorani v State of Bihar 2003).

60 Illustratively, the number of complaints made to data protection authorities has increasingly demonstrably (Whittaker 2018), (Anonymous 2019) and (Kalman 2019).

concerned. The vulnerability of users therefore does not stem organically "from the structure and nature of the fiduciary relationship" (Khan and Pozen 2019).

While one cannot disagree with the main thrust of this argument, one does wonder whether this should in itself see rejection of the information fiduciary concept.[61]

First, user's typically have little to no choice regarding the selection of online services or indeed the types of information that may be captured about them. The power imbalance in relationships with data processing entities can arise from mere use of the service - and not only the activities of digital companies in collecting excessive data or driving addiction, etc. Even if the digital economy were not monopolised and service providers did not collect such large quantities of personal data, this would in no way take away from the need to ensure that personal data, in whatever amount, was not misused or used against the interests of users.[62]

Second, often, the more the information provided by the user, the better the nature of service. This can be seen as akin to that of a doctor-patient relationship. There may be some basic information that the doctor requires to treat a patient but receiving more information may help the doctor better diagnose the ailment and suggest more appropriate treatment.

Finally, Indian courts have recognised the existence of a fiduciary relationship largely on the basis of the vulnerability in the relationship and trust that data will be kept confidential (i.e. whether the information was private in nature and therefore carried an expectation that it would be kept confidential).[63] The fact that the fiduciary and non-fiduciary parts of a relationship can also be separated in Indian law would appear to indicate that in certain contexts mere information

61 Accessing services for free in exchange for data can be a legitimate user choice, assuming it is made with informed consent. For instance, if a doctor decides to provide free services to a patient in exchange for the ability to sell the patient's data to a medical research institute one could see such a relationship being permitted even within the bounds of a fiduciary relationship subject to patient consent, a level of certainty about the downstream uses of data, etc.

62 Note that Indian courts have held that fiduciary relationships can be confined to particular acts or actions and need not manifest themselves in the entirety of interaction or relationship between the parties (Union of India v. Central Information Commission 2009).

63 See for instance, (The Institute of Chartered Accountants of India v. Shaunak H Satya and Ors. 2011), where the court held that an examining board was in a fiduciary relationship with its examiners in respect of information exchanged between them on how exams were to be marked. See also (M. Kanniyappan vs. The Presiding Officer, Labour Court and Ors. 2011) and (Raju Sebastian and Ors. v. Union of India and Ors. 2019).

exchange can indeed lead to sufficient vulnerability so as to qualify the relationship as fiduciary.

- **Choice of fiduciary:** In traditional fiduciary relationships, obligations are only imposed on the fiduciary pursuant to consent to undertake the various onerous duties required by the relationship. In the case of certain entities involved with data processing, the data processing entity may not have a practical choice in terms of denying the user access to services. This is particularly true of essential or public utility services, including for instance telephone and internet service providers.

Overall, it appears that digital service providers can certainly be in a position of power with respect to users by virtue of the information that users have to provide to avail their services, and the absence of any real user choice to use their services. Users do tend to expect their data to be used in certain limited ways, and in any event, not to disadvantage them or cause them harm.[64] The power enjoyed by these entities can be unilaterally exercised so as to affect the rights and interests of the user (in the form of disclosure, acting on the basis of user profiling, etc.) and there is a social need for protection of user interests in such cases. The information asymmetry in such relationships, in addition to other issues such as the technical and structural concerns of the digital ecosystem, also make it difficult for users to either rely on contract, consumer protection or tort law, etc. to seek remedies. The information asymmetries problem in particular limits the abilities of users to act as autonomous and informed agents while contracting or indeed seeking remedies. The fiduciary concept could therefore prove useful in protecting user rights in the digital ecosystem.

Some, if not many relationships that involve processing of personal data, would not normally fall within the scope of the fiduciary concept. However, there is no reason why statute cannot deem certain relationships as being akin to fiduciary relationships, and thereby bring within its scope all necessary actors in the digital ecosystem (with relevant exceptions, based on social need and risk of harm). Duties can then be imposed that are similar to those in a fiduciary relationship should this be felt necessary to solve a

64 This is true not just in the US but also India. See for example (Punia, Kulkarni, and Narayan 2019).

particular social problem. The existing body of law pertaining to fiduciaries can become a useful tool in interpreting the scope of the duties created by statute.

3.3. Duties of information fiduciaries

By virtue of digital service providers being treated as information fiduciaries, they will be required to undertake certain duties towards their users. As with traditional fiduciary relationships, Balkin proposes basic duties of loyalty and care, together with certain additional duties designed to limit the agency problem in the relationship.

The standard of loyalty and care Balkin crystallises for information fiduciaries is that they should not be allowed to act as con-artists i.e. induce trust in their end users to obtain personal information, and then betray end users or work against their interests (J. M. Balkin 2016).[65] Balkin believes that the duties of online service providers should be of a lesser standard than those imposed on traditional fiduciaries.[66] He therefore proposes a 'good faith' standard rather than 'best interest' or 'sole interest', which he argues, could effectively prohibit many data driven business models.[67]

Specifically, he proposes the following set of obligations that information fiduciaries can choose to implement under the terms of his "grand bargain":

- to institute a set of fair information practices (to set expectations of users and reduce information asymmetry),
- disclose data breaches (to reduce information asymmetry),

65 Betrayal of trust would occur when the fiduciary acts in an unexpected way or breaches some other socially important norms.

66 This is justified on three grounds: first, they rely on monetising user data to drive their profits. By applying fiduciary duties, the idea is not to make these companies into not-for profits; second, users dont expect the same standard of care from such entities as doctors and other such relationships; and third, service providers have an interest in ensuring greater use of their services and no positive obligation not to do so. (J. M. Balkin 2016).

67 A good faith standard implies that parties must act reasonably, honestly, fairly, with due care and attention. Such a standard has been said to impose an obligation on the parties to observe reasonable commercial standards of fair dealing, to observe faithfulness to an agreed purpose and display consistency (Berkeley Community Villages Ltd and Anr. v Pullen and Ors. 2007). It has been termed as being akin to "playing fair", "coming clean" and "putting one's cards on the table" (Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd 1989). A best interest or sole interest requirement could imply that the fiduciary cannot profit from data at all and any processing would exclusively have to be in the interests of the beneficiary. Monetisation of personal data would therefore become difficult with such a high standard, though rights protection would certainly improve.

- promise to not leverage personal data such that it leads to unfair discrimination or abuse of trust of end users (to preserve duties of loyalty and ensure adherence to expectations of users),
- agreeing not sell or distribute consumer information except to those who agreed to similar rules (to preserve duties of loyalty and care).

These duties are elaborated by (Dobkin 2018). Using the basic test of whether a practice is acceptable or not, based on a user's expectations, she suggests four principles around which the duties of an information fiduciary could be framed.

- *No manipulation of the user:* This principle prohibits service providers from using information about users to surreptitiously manipulate them.[68] Manipulation of a user is said to breach fiduciary responsibilities as users are both unaware of and do not expect such activities. Covert action exploits information asymmetry and place the fiduciary's interests above the beneficiary's.
- *Antidiscrimination:* The second principle prohibits discrimination against users.[69] As in the case of manipulation, discriminatory actions by service providers can be said to generally violate user expectations. Users are in no position to either understand or consent to such practices.
- *Limited sharing with third parties:* The third principle involves limiting data sharing with third parties.[70] Dobkin argues that unless all third parties are also considered information fiduciaries towards the users, sharing data with them should be considered a violation of the information fiduciary's duty.[71]

68 Manipulation has been defined as an action or statement that *"does not sufficiently engage or appeal to people's capacity for reflective and deliberative choice"* (Dobkin 2018).

69 The term is used widely so as to go beyond merely traditional concepts such as race, color, religion, age, nationality etc.

70 Users may not trust downstream processors of data to the same extent as the entity they provided the information to, and as privacy policies tend to be unclear on who data will be shared with and in what form.

71 However, she argues that there are certain types of companies which cannot be considered information fiduciaries at all. These are data brokers who buy data to create fuller profiles of consumers and then sell it further. Users would not willingly give data to such companies. Therefore, according to her, no fiduciary should share or buy data from companies which are based on business models of buying data from many sources to create fuller profiles of consumers.

- *Prohibition from violating company's own privacy policy:* The final principle involves the need for the company to follow to its own privacy policy - since this is the basis on which user expectation is created.[72]

The duties prescribed by Balkin and Zittrain and built upon by Dobkins appear to cover some of the most pernicious practices undertaken by digital entities. The duties of ensuring obligations flow with the data and to adequately disclose information - including by way of data breach notifications - are particularly noteworthy. That said, the range and scope of duties is open to question on the grounds discussed below.

3.3.1. Does the concept adequately protect users?

The information fiduciary concept applies to information provided in private settings and with an expectation of privacy *at the time* it is provided.

The reliance of the concept on the expectations of users as a standard to gauge the validity of practices can be problematic. It has been argued for instance, that such a concept lacks any independant normative standard and therefore does not adequately protect privacy rights (Crowther 2012) and (Schneir 2009). Balkin himself notes that essentially the standard he proposes would require users to factor the monetisation of their data into account (J. M. Balkin 2016). This may not be possible for all users. Expectation and reasonableness based standards are also said to disproportionately impact vulnerable sections of the populace, who may in fact require stronger privacy protections (Gellman and Adler-Bell 2017). It should also be considered that certain types of data - such as names, faces etc., may be publicly used by individuals but still carry some expectation of privacy dependant on the context. For instance, you may post pictures freely on Facebook but may still not want the company to use this for certain purposes such as identifying you automatically in pictures posted by other users, or sell such data to third parties, etc. The fiduciary concept could have trouble dealing with such instances, as typically only appears to protect information that is not "public" in nature.

72 Dobkins suggests imposing minimum standards against which privacy policies should be measured. Information fiduciaries should be required to provide clear disclosures in a manner understandable to an average user, and in a manner that enables users to understand how their data might be used.

Given that the concept only applies to data exchanged in private settings, an individual's privacy rights over data can end if voluntarily placed in the public domain at any point of time. However, data protection regimes such as the GDPR continue to recognise certain individual rights over personal data even once made public - for instance, by recognising a right to forget.[73] The information fiduciary concept appears to lack the ability to provide such level of rights protection.

Further, while the concept could, it has not been extended to cover other obligations/ rights recognised in modern data protection laws such as data portability rights (which can enable users to control their relationships with service providers) or even by giving fiduciary's the responsibility to represent the beneficiary's interests while say resisting calls for information from law enforcement agencies.[74]

As mentioned previously, concerns about the workability of the notice-consent framework will also remain. User's may simply not read privacy policies or be able to adequately evaluate risks involved (despite the data processing entity concerned taking reasonable steps to permit them to do so). As Khan and Pozen point out, the nature of information asymmetry in the digital ecosystem is of a significant order. It could therefore be argued, that just as trust relationships often do not permit the beneficiary to consent to certain harmful acts (say where incompetent to contract, or where the risk of harm is significant as in the case of a beneficiary's interest being bought by the trustee) there is a need for higher standards of care to be imposed.[75]

However, the duties described previously need not be the only mechanisms for implementation of the concept or indeed the exact standard required to be adopted by law.

73 Under this right, data once made public can, under certain circumstances, be made private once again (when privacy interests trump freedom of speech interests).

74 Similar to how Section 702 of the American Foreign Intelligence Surveillance Act permits electronic communication service providers to file petitions before the Foreign Intelligence Surveillance Court to set aside or modify directives to assist or provide information to law enforcement authorities.

75 The standard of consent prescribed becomes important particularly as industry practice may significantly diverge from public expectations, not least due to the fast development of technology and the inherently non-transparent nature of digital products and services.

The range of rights and remedies suggested by Balkin could be strengthened, as has been done with the two American laws described later on in this paper.[76]

3.3.2. Does the concept merely replicate existing legal standards?

It is argued that existing law - whether in contract or consumer protection law - already requires companies to adhere to standards of fair dealing and good faith and restrains them from acting as con-men (Khan and Pozen 2019). This has lead to privacy related actions being initiated against companies such as Google and Facebook (Khan and Pozen 2019).

In the Indian context, this argument appears even stronger given the presence of Section 88 of the Trusts Act, which protects beneficiaries in any relationship considered by the court to be of a fiduciary character. It is therefore already open to users to use this provision to proceed against data processing entities for breach of fiduciary duties, though they would first have to establish the relationship as being fiduciary in character.

Existing law does indeed give consumers some remedies against privacy invasive practices. However, the standard of care and the range of rights/obligations in Indian law contract and consumer protection law are significantly limited. While current Indian law does prevent fraudulent behaviour, contract law does not include an express "good faith" requirement as US law does.[77] Consumer protection law too only protects consumers from certain limited harms such as those defined as "unfair trade practices". The recognition of a fiduciary standard can therefore improve rights protection in India by raising the standards of care from that in existing law.[78] The fiduciary concept

76 The scope of duties can be further stregthened from Balkin's standard including to the extent that service providers may have to function more or less as charities. For instance, imposing a "manifestly beneficial", "sole interest", or "utmost care" standard could be interpreted to mean that all data monetising practices that do not confer an exclusive benefit to the beneficiary could be deemed illegal. The remedies he proposes (such as the use of voluntarily mechanisms based on safe harbour being provided under a "grand bargain") can also be ignored in favour of more typical deterrance based enforcement mechanisms.

77 In the American context refer to Sections 1-304 of the American Uniform Commercial Code and Section 205 of the Restatement (Second) of Contracts. See also (Dubroff 2006). In the Indian context, the Contract Act recognises such a duty in only certain limited cases (see Section 223, Indian Contract Act, 1872). Insurance contracts have an "utmost good faith" requirements as per which all material facts must be disclosed (Makkar 2018) and (Law Commission of India 2006). Note that the Law Commission of India has its 199th report, suggested reforming contract law standards to include requirements of substantive and procedural good faith (Law Commission of India 2006). No action appears to have been taken on the Law Commissions said recommendations.

78 In addition to the low standards, individuals are also likely to face problems pertaining to evidentiary issues and demonstrating harms and damage. See generally (Law Commission of India 2006).

also allows imposition of ex-ante measures, which are essential in the privacy context (as harms can be serious and permanent in nature).[79]

3.3.3. Does the concept fail to address structural problems?

Khan and Pozen argue that the information fiduciary concept fails to deal with more important structural problems associated with the digital ecosystem such as problems associated with monopolisation, the effects of behavioural advertising on users, and the problems of online speech. They point to how the relatively low standard of care proposed by Balkin (despite the fiduciary nature of the relationship), could strengthen existing business practices (such as profiling and behavioural advertising) rather than act to ameliorate their dangers.

The standards of care and range of duties proposed by Balkin are indeed not of the highest order. These limitations however are not terminal to the concept itself. Fiduciary law, in theory, allows varying degrees of obligations to be imposed. The low standard chosen by Balkin is on account of his interest in protecting business models of corporations. In addition to enhancing the standards of loyalty and care, the concept also permits other obligations such as the right to forget or a right to data portability to be read into the scope of fiduciary obligations.

At the same time, implementing fiduciary duties on data processing entities does not imply a reduced need to engage in competition law reform, regulation of online speech or any other attempts at regulating the assorted forms of harm occuring in the online environment.[80] Keep in mind that competition law may also struggle to adequately deal with the problems of the digital ecosystem for example, due to the presence of strong network effects and the difficulty in imposing interoperability regimes to digital services.

79 Contract and consumer protection law have limited, post facto remedies that primarily aim at restitution. Fiduciary law aims at preventing breach through deterrance.

80 Further, while the concept primarily tries to address a limited range of privacy related harms, it has also been extended to other contexts such as pertaining to the ethical uses of the AI and machine learning (Pasqual 2017), (J. Balkin 2018) and (Lightbourne 2017).

3.4. Applying the information fiduciary concept (in the US)

Balkin's thesis has received acclaim in both the media and amongst academics.[81] The US has also seen the introduction of two proposed laws based on this concept - the New York Privacy Act at the state level, and the Data Care Act at Federal level. We briefly examine how the information fiduciary concept is applied in these laws.

3.4.1. Privacy Act, New York

The New York Privacy Act was introduced in the state senate in May 2019.[82] The law imposes fiduciary duties of loyalty and care on data processing entities[83] and obliges companies to "act in the best interests of the consumer, without regard to the interests of the entity…in a manner expected by a reasonable consumer under the circumstances". Interestingly, the law specifically mandates that fiduciary duties towards the user should trump the company's fiduciary duty towards shareholders.

In order to fulfill their fiduciary obligations, companies are required to *inter alia:*

- secure personal data from unauthorised access and inform users in case of data breaches;
- refrain from using personal data (or data derived from personal data) in a way that will "benefit the online service provider to the detriment of an end user" and will result in "reasonably foreseeable and material physical or financial harm to a consumer" or that "would be unexpected and highly offensive to a reasonable consumer";
- ensure data protection obligations flow with the data when it is shared;
- refrain from data processing and transfer without express consent;

81 It has for example, been described as "well developed and hard to challenge" (Pasqual 2017), and a concept that can make "Facebook and Google behave" (Editorial Board 2018).

82 The law is currently being discussed in the senate consumer protection committee (New York State Senate 2019). News reports however indicate that substantial lobbying efforts (in particular by businesses) have lead to the law being shelved (Ropek 2019) and (Yannella 2019).

83 This is done by mandating that any data processing entity is "to exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk". The law recognises a range of risks that users must be protected from. This includes direct and indirect financial losses, physical and psychological harm (such as anxiety, embarassment, fear, mental trauma, etc), significant inconvenience, reputational harm, price discrimination, and any adverse consequences related to a user's legal benefits.

- be transparent and accountable to users including through informing them of the existence of user rights, the categories of data that will be processed, disclosing any profiling practices and consequences thereof, providing information on methods of de-identifying personal information, uses to which personal data will be put, the entities with whom data will be shared, etc.

Users are given the right to approach courts for breach of a company's duties, and there are no limitations to the fines that can be imposed.[84]

The law therefore imposes a range of fairly stringent measures on data processing entities - arguably, greater than that envisaged by Balkin. In addition to casting specific duties of loyalty and care on a wide range of data processing entities (much broader than that conceptualised by Balkin), the law clarifies that companies are not to engage in acts that could lead to a series of widely defined risks.

Crucially, they are not to engage in acts that could be interpreted as leading to their own benefit at the cost of the end-user. In addition to putting place restrictions on usage of personal data itself, the law also recognises that harms that could be caused to users through data derived from personal data and therefore also imposes obligations in this respect. This could be seen as an extension or strengthening of the loyalty rule - in that companies are limited from profiting from their user's data in any way at all, directly or indirectly.

3.4.2. Data Care Act

The Data Care Act, is largely similar to the New York law described above, though it is more limited in scope. It seeks to apply fiduciary duties to a specific class of data processing entities by establishing duties of care, loyalty and confidentiality.[85]

84 Courts must consider the severity of the violation, the extent of harm caused and revenues of the company concerned, when deciding the quantum of compensation.

85 The law, introduced in the US senate in December 2018, applies to "online service providers" and "any other digital networks". Further, being a federal law, it only applies to activities involving inter-state commerce. The duty of care envisaged in the law encompasses obligations to secure personal data from unauthorised access and notify users of breach. The duty of loyalty obliges service providers to refrain from using personal data (or data derived from personal data) in a way that "will benefit the online service provider to the detriment of an end user and will result in reasonably foreseeable and material physical or financial harm to an end user or would be unexpected and highly offensive to a reasonable end user". The duty of confidentiality places restrictions on data sharing.

The law envisages State Attorneys, State Consumer Protection Officers and the Federal Trade Commission as enforcing agencies - i.e. they can bring actions against companies for breach.[86] It imposes various civil penalties on defaulting entities based on the harm caused to end users, subject to certain maximum limits.

This law therefore is more limited than the New York law - in terms of its applicability, the specific obligations imposed on data processing entities, its recognition of specific harms, as well as the possible remedies available to users. Notably, users cannot directly approach a court for relief. Nonetheless, this law too specifically recognises that service providers must place the user's interests before their own and must generally act in a faithful, transparent and accountable manner.

4. Fiduciary relationships under the draft Personal Data Protection Bill, 2018

In this section of the paper we first attempt to understand how the Justice Srikrishna Committee conceptualises a fiduciary relationship in the data protection context. We then examine the obligations imposed on data fiduciaries under the PDP Bill to understand how the draft law addresses the agency problem in the data principal-data fiduciary relationship. Are the obligations imposed under the PDP Bill comparable to the obligations imposed on traditional fiduciaries? Next, we examine whether the PDP Bill uses the fiduciary concept to approach the issue of data protection in a novel manner. We undertake a summary comparison of the obligations imposed by the PDP Bill and the GDPR to see whether the PDP Bill imposes obligations beyond those imposed in nonfiduciary based data protection models. We conclude with comments on the effects of the fiduciary framing in the draft PDP Bill.

86 It also permits the Commission to exempt certain entities from compliance based on the privacy risks posed by the entity and the costs and benefits of regulating the entity.

4.1. Conceptualising "data fiduciaries"

In its Report, the Justice Srikrishna Committee seeks to marry the twin objects of protecting individuals from privacy related harms caused by state and non-state actors, while also enabling growth of the digital economy (Government of India, Ministry of Electronics and IT 2017).[87] The Committee highlights two factors that it believes can lead to the creation of a "common public good of both a free and fair digital economy" - first, enhancing the autonomy of individuals to regulate processing of their personal data, and second, developing a regulatory framework where the "inequality in bargaining power between individuals and entities that process such personal data is mitigated" (Justice Srikrishna Committee 2018).

The Committee eschews the commonly used phraseology in various data protection laws[88] of a "data subject"[89] and "data controller".[90] Instead, it introduces the terms "data fiduciary" and "data principal", in an attempt to re-cast the data subject-data controller relationship as a classic fiduciary-beneficiary relationship.

Per the Committee, the purpose of such a framing is to try and place the interests of the data subject at the centre of the data protection framework given: first, the inequalities in the relationships between data subjects and data controllers, second, the dependence of the data subject on the data controller, and third, the possibility of abuse of power by the data controller.[91]

The Committee seeks to reduce this seeming vulnerability by elucidating a range of statutory rights and obligations applicable to data principals and data fiduciaries respectively. These rights and obligations are based on the understanding that individuals share personal data with entities based on a fundamental expectation of trust and

87 The White Paper released by the Committee states that the objective of the exercise is "to ensure growth of the digital economy while keeping personal data of citizens secure and protected" (Justice Srikrishna Committee 2017).

88 For example, the General Data Protection Regulation, various local legislations in European countries such as the UK's Data Protection Act of 2018, Brazil's General Data Protection Law of 2018, South Africa's Protection of Personal Information Act (which however refers to a data controller as a "responsible party"), etc.

89 Denoting the individual whose personal data is the subject of collection and processing.

90 Implying the entity determining the nature and means of processing of a data subject's personal data.

91 The Committee observes that existing data protection frameworks that designate the individual as "data subjects" often place the interests of the individual whom the data pertains to, after that of companies that deal with such data.

loyalty. Accordingly, the Committee believes that a duty of care ought to be placed on entities collecting and processing data to:

- act fairly and responsibly,
- for purposes reasonably expected by the data principals, and,
- in the best interests of the data principal.

This does indeed accord with the general understanding of the fiduciary concept discussed in the first section of this paper and indeed echoes the concept as outlined by Balkin.

However, the Committee doesn't consider if all relationships in the digital economy are as one sided - whether the nature of vulnerability and trust (in all cases of personal data processing) is comparable to traditional fiduciary relationships, whether all data processing entities provide expert, professional or personalised services or indeed whether a generally recognised duty of loyalty exists in all relationships of information exchange. The Committee relies on the fact that information exchange *alone* can lead to vulnerability between parties, and can shape the reasonable expectations of individuals.[92]

This tweaking of Balkin's concept is made easier by the fact that Indian constitutional law balances speech and privacy rights. This means a greater ability of the state to restrict speech rights, implying that the PDP Bill does not *have* to view data processing entities as fiduciaries in order to regulate them. As a consequence, the PDP Bill also evades the problems with narrowness of Balkin's conception of information fiduciaries. The scope of the concept is then statutorily reduced through exemptions. The scope of the concept is also restricted to cover only "personal data" - thereby avoiding an expansion into areas such as data derived from personal data or non-personal data collected from individuals. Expansion into such areas would not violate the fiduciary

92 The Committee notes that users may expect different levels of trust and loyalty from different data fiduciaries based on the natue of data, purposes of processing and entities with whom data will be shared. The Committee does not go into the issue of the degree of vulnerability or expectation created in a data fiduciary-data principal relationship.

concept, but would enable users to, for instance, claim from service providers if their personal data is used to produce insights used in building AI based products (thereby possibly restricting business interests).

It is also worth noting that the fiduciary concept is largely used in circumstances where it is necessary to protect one party against another due to the vulnerability in the relationship. The beneficiary's interests are always protected against the fiduciary. The data protection context however often requires a balancing of interests, rather than one interest being privileged over the other. In that sense, the choice of a fiduciary framing may be considered inappropriate for a comprehensive privacy legislation which must cover numerous types of processing where the individual's privacy interest may not necessarily require top priority.

Generally speaking, use of the fiduciary framework would make sense in two circumstances:

- if it is used to raise the standards of obligations imposed on data processing entities beyond that typically seen in data protection laws (say, those based on notice-consent or on fair information practices), if it adds anything novel to typically seen data protection obligations or if it provides a new way to balance competing interests in the data protection ecosystem;
- if it enables one to implement privacy regulation while avoiding constitutional hurdles (as is the case with the US).

Given India's constitutional framework does not necessitate a fiduciary framing to avoid constitutional roadblocks, it makes sense to use the fiduciary framing if the concept would allow novel data protection related obligations to be imposed. As indicated in the previous sections of this paper, the fiduciary concept can indeed cast a high standard of obligations on entities brought under this framework (that can go beyond typically seen data protection obligations). For instance, the two draft US laws described in the previous chapter both cast specific and high standards of loyalty and care on data controllers. These restrict the ability of the data processing entity to carry out certain types of processing that can be seen as being against the

individuals interests/benefiting the data controller at the cost of the individual, and thereby go beyond typical obligations seen in data protection laws.[93] The fiduciary concept can then be used to allow adjudicatory authorities/courts to decide if a particular practice breaches the prescribed standards of behaviour.

We therefore turn to two issues: first, whether the scope of duties imposed under the PDP Bill are indeed 'fiduciary' in nature (when compared to obligations expected of traditional fiduciaries), and second, whether the use of the fiduciary concept in the PDP Bill goes beyond non-fiduciary based privacy frameworks such as that used in the GDPR.

4.2. Are the duties under the PDP Bill 'fiduciary' duties?

As mentioned previously, the primary interest in utilising the concept of a data fiduciary in the framework set out by the Committee is to prevent the possible abuse of power that a data fiduciary has over a data principal.[94]

To eliminate or reduce the possibility of such an abuse of power, the draft PDP Bill: (a) casts a generic obligation on all data fiduciaries to process personal data in a "fair and reasonable" manner;[95] (b) lays out numerous specific measures that cast a duty of care on data fiduciaries. Breach of the prescribed duties leads to a cause of action against the data fiduciary, (c) empowers the data protection authority to bar specific data processing practices if found to be likely to cause harm to the data principal.[96]

We now discuss these obligations and how they compare to the duties typically expected of fiduciaries.

93 The extension of obligations to cover derived data and the wide scope of remedies are also noteworthy in this respect.

94 The Report understands an 'abuse of power' as taking place when personal data is not processed in an authorised manner, and for ends that may not be in the data principal's best interest (Justice Srikrishna Committee 2018).

95 Section 4, draft PDP Bill.

96 Specific processing practices may be barred by the data protection authority under Section 33(5), if the authority believes the practice is likely to lead to harm (upon scrutiny of a data protection impact assessment submitted by the fiduciary). The requirement to conduct such an assessment arises either where the processing activity in question raises a risk of "significant harm" or where otherwise required to do so by the authority.

4.2.1. Fair and reasonable processing

The obligation to ensure "fair and reasonable" processing acts as a overarching requirement for all entities engaged in processing personal data. Per the Committee, this requirement for "fair and reasonable processing" implies:

1. the processing must be such as can be reasonably expected by the data principal;
2. while processing of personal data ought to be based on a recognised ground, this may not always be sufficient to constitute "fair and reasonable" processing;
3. consent may not always be a sufficient ground for a data fiduciary to disclaim liability;
4. obligations on a data fiduciary would be passed on to an entity carrying out processing on its behalf (irrespective of a direct relationship between the data principal and the data processor).

By requiring the data fiduciary to inform the data principal of relevant processing practices, and making it mandatory for processing to be fair and reasonable, the legislation appears to impose a "good faith" standard (similar to American contract law).

This standard of loyalty/care is however not the highest possible. There is no general requirement in the PDP Bill for the data fiduciary to act in the user's interests, for their benefit or to avoid acting in a manner detrimental to the user.[97]

"Predictability" of processing is not synonymous with processing in the data principal's "best interest", "sole interest", or even to act "for the benefit" of the beneficiary. Though the Committee repeatedly recognises the need for data fiduciaries to act in the "best interests" of the user, this standard is not explicitly included in the law with the general

97 As discussed in the first section of this paper (and in Annexure - I), laws pertaining to directors, doctors and particularly trusts, all contain provisions specifically limiting the ability of a fiduciary to act in their own interests or against that of the beneficiary.

standard applied in the PDP Bill only requiring data fiduciaries to act in a bona fide, diligent and reasonable manner.[98]

The good faith standard is certainly an improvement on current contract and consumer protection law in India, but only implies that data processing entities will be required to refrain from acting in a manner that can be considered as being mala fide or against principles of fair dealing. They will be required to make all material disclosures, not trick users or claim one thing and do another. In general, practices such as targetted advertising, profiling, use of personal data for AI development, etc. will continue to be permitted though subject to specific disclosure and consent requirements (amongst other requirements under the statute).[99]

This is similar to the standard currently applicable in India with respect to insurance contracts (Makkar 2018). Further, this standard is similar to that found in contract law in countries such as that in Germany, Netherlands, Italy and the United States (which require fair dealing and acting in accordance with reasonable practices).[100]

As recognised by (Langbein 2005), a lower standard is generally used where it is easier to overcome information asymmetry problems or where social norms otherwise dictate

98 Notably, the PDP Bill itself uses the phrase "best interest" only once - in the context of protection of children's data. By way of comparison, the Report of the Committee uses the phrase five times - in the context of processing of data of children (internal page 44), while explaining the scope of the duty of care (internal page 51), twice while explaining the obligation to process fairly (internal page 52) and while summing up the obligations cast on data fiduciaries (internal page 66). The requirement to act in the "interest" of the data principal too is largely missing from the draft law a few sections excepted. Therefore, Section 29 pertaining to the implementation of privacy by design requires data fiduciaries to implement policies and measures to ensure *inter alia* that "the interest" of the data principal is accounted for at every stage of processing, Section 60 empowers the data protection authority to "protect the interests of data principals", and Section 64 empowers the authority to inquire into processing practices that are "detrimental to the interest" of data principals.

99 The Report of the Committee recognises that data fiduciaries should be prohibited from engaging in practices such as behavioural monitoring, tracking, targeted advertising, etc., insofar as these practices pertain to children (as these go against the best interest of the child).

100 Refer Burgerliches Gesetzbuch (BGB), 1900, § 242; Italian Civil Code, 1942, Art 1137; Niew Burg-erlijk Wethoek (NBW), 1992, and Uniform Commercial Code (U.C.C.), 1990, § 1-203. The standard has also been read into Indian contract law in at least one case (Association of Unified Telecom Service Providers of India v. Union of India 2014). As noted previously, the Law Commission has recognised the need for Indian contract law to also include provisions requiring procedural and substantive good faith in contracting. Notably, the Law Commission has recommended treating contracts that lead to an unfair advantage to one of the parties, in view of the circumstances of contracting as voidable. In considering the nature of "unfairness", courts are to *inter alia* consider factors such as the knowledge of the promisee in relation to the meaning and effects of the contract, the relative bargaining strength of parties, reasonable standards of fair dealing, whether contractual terms were in fine print or easy to read and understand, etc.

the need to do so. Accordingly, this lowering of standard can be traced to the Committee having to balance business and individual interests.[101] The PDP Bill therefore attempts to find a middle ground by imposing requirements to act in accordance with generally expected practices, but not specifically restricting all potentially risky or injurious practices altogether.

It is unclear if this is a sufficient standard of rights protection in the data protection context in view of the various consent related problems in the digital ecosystem and the vast information asymmetries present in a country like India (Punia, Kulkarni, and Narayan 2019), (Bailey, Parsheera, Rahman, and Sane 2018) and (Matthan 2017). On the other hand, by imposing such a standard, the Committee puts the onus on individuals to take charge of and actively seek to protect their privacy rights (as opposed to being viewed through paternalistic eyes).[102] Further, the safeguard of the data protection authority being able to step in and prohibit/seek modification of any particularly problematic practice acts as a check on the most pernicious practices of large data processing entities.

As demonstrated in (Bailey, Parsheera, Rahman, and Sane 2018), individuals may indeed be able to understand privacy policies given optimal conditions, including sufficiently clear information.[103] However, in this context, (Khan and Pozen 2019)'s perspective on the need for structural change in the digital economy take on added importance. Users have limited choice of services in the digital economy (particularly in areas where network effects and economies of scale may be particularly large). Therefore even if informed of harmful practices by data fiduciaries, they may have no choice but to accept them.

A truly fiduciary standard would have an explicit requirement for the fiduciary to place interests of the beneficiary first (such as in the case of the two American laws discussed previously or indeed as the PDP Bill itself does in the context of children). It would not

101 This is similar to Balkin's framework where he is wary of placing a very high standard of loyalty on data fiduciaries that could force them to act virtually as charitable institutions (J. M. Balkin 2016).

102 This is akin to why doctors are not considered fiduciaries in common law in England. Indian law does however recognise more paternalist duties of doctors including in the requirements of disclosure and consent.

103 Further, and as mentioned previously, certain particularly risky practices can be barred by the data protection authority. While this may limit the autonomy of the individual, it would act to protect against the most pernicious data processing harms.

allow contracting out of situations where the data principal's interests are not always placed over that of the data fiduciary, or would make this extremely difficult.[104] Such a standard would raise the level of rights protection, but limit business interests. Even the ability of the data protection authority to bar certain practices that cause harm does not exactly correspond to a requirement to act in the beneficiary's interest or to its benefit. This standard would give business entities greater leeway in their processing activities (the standard of acting in a beneficiary's interest or for its benefit being higher than a requirement not to cause certain specific harms).

The PDP Bill also does not explicitly bring derived data within its scope. Derived data will only be protected if it falls within the scope of personal data i.e. if it can be reasonably traced back to the individual. The fiduciary concept would in theory even allow even non-personal data to be protected as long as provided to the fiduciary in a context where confidentiality is expected. This is seen for example, in the case of the two American laws referred to previously.[105] Companies in India will therefore be able to continue to use non-identifiable derived data for their business purposes even after withdrawal of consent by the data principal.

Further, full use of the fiduciary concept could permit the data principal to exercise claims over even the products of processing personal data - by imposing sufficiently high standards of loyalty and using principles pertaining to that of a constructive trust, tracing/conversion. The PDP Bill does not extend to such lengths given its focus on balancing business needs with privacy rights.

4.2.2. Purpose limitation

The central idea behind the PDP Bill is to ensure data principals have greater control over how their personal data is used. One of the ways this is achieved is by limiting the uses of personal data to those purposes which the data principal is specifically and

104 While in traditional fiduciary relationships informed consent can be used to waive or reduce the duties of loyalty and care, these law also impose a host of safeguards to prevent against abuse. These usually take the form of specific disclosures, and in cases where consent is deemed impossible or insufficient, as in the case with minors in the case of trusts, courts are permitted to step in and act in their interests.

105 In order to seek protection of non-personal data using the fiduciary concept, the user could still proceed under existing law (say under the Trusts Act).

clearly informed about, or for purposes incidental thereto.[106] Essentially, data fiduciaries must ensure that their user's expectations are appropriately established through proper disclosures. Users will then have the option of consenting to or denying a particular practice.

4.2.3. Consent

The concept of individual consent is central to the draft PDP Bill. Section 12 of the draft law recognises consent, given no later that at the time of commencement of the processing, as a valid ground for processing of personal data.[107] The draft law also recognises a higher threshold of consent for processing of certain categories of data categorised as "sensitive personal data".[108] Data principals must also be given the right to withdraw their consent (subject to taking on any legal consequences for such with-drawal).[109]

The Bill does not specifically circumscribe the ability of the individual to consent to activities that may not necessarily be in his or her interest. For instance, the Bill permits processing even where there are risks to the data fiduciary - just as long as explicit consent is secured.[110]

This above is not per se against the fiduciary concept, though, as noted previously, both academics and courts appear to be hesitant about recognising the entirety of a fiduciary relationship to be voluntary/subject to contractual waivers.

106 Section 5 of the PDP Bill.

107 In order to be considered legitimate, all data processing must be based on a valid ground. The draft Bill recognises 6 specific grounds for processing - consent and 5 other grounds for non-consensual processing.

108 In such cases, it would be necessary for the data fiduciary to secure "explicit consent". Section 18, draft PDP Bill.

109 Section 12, draft PDP Bill.

110 Note that the data protection authority is empowered to prohibit certain processing practices or impose relevant conditions on the same, in the event the data protection impact assessment carried out under Section 33 of the draft law leads the authority to believe that any processing practice is likely to cause harm to the data principal. Such an assessment is to be carried out in cases where the processing carries a risk of significant harm to data principals such as where there is large scale profiling or use of sensitive personal data, or the processing involves new technologies. In so far as a practice is not specifically barred by the data processing authorities, entities may continue to indulge in the same even if not entirely in the interests of the data principal.

It therefore becomes critical that the PDP Bill implement appropriate safeguards to ensure that consent is only considered valid when the beneficiary is provided sufficient information so as to enable an adequate understanding and assessment of all the risks involved.

To this end the draft Bill does ensure that for consent to be considered valid, it must be free, informed, specific, clear and capable of being withdrawn. The onus is also placed on data fiduciaries to provide relevant information in their privacy policies in an accessible way and thereby set the expectations of data principals appropriately.[111]

The law therefore uses an "informed consent" standard, a standard used in case of doctor-patient relationships in the US (Canterbury v. Spencer 1972). This has been interpreted as a requirement to inform the beneficiary of "all the risks potentially affecting the decision".[112] The data fiduciary would not really have discretion in the provision of information - it would have to give any information that could be reasonably required by the data principal to make a choice.[113] The standard is therefore of a high order.[114]

Accordingly, one may expect adjudicatory authorities to set aside practices where insufficient information is provided or information is provided in an unclear or inaccessible fashion, such that a reasonable man would not be able to fully understand the consequences/effects/harms of assenting. The onus will be on the fiduciary to show that the practice was clearly explained. Should companies provide an explanation, in

111 Further, data fiduciaries cannot make consent to any unconnected data processing a condition precedent to offering any services to an individual. The data protection authority is also empowered to notify consent forms to be used by different types of services. Adhering to them will automatically imply adherence to the notice related provisions in the law. The law therefore precludes the possibility of any challenges based on individual circumstance. This enables certainty for business though possibly at the cost of vulnerable users (who may find it difficult to engage with privacy notices, as compared to more advanced users who are likely to be closer to the "objective" reasonableness based standards in the law.

112 See (Canterbury v. Spencer 1972), (Reibl v. Hughes 1980) and (Rogers v. Whittaker 1992).

113 The PDP Bill however limits the information provision requirement to the categories specified under Section 8 of the law.

114 It is notably higher than a "valid consent" requirement as used in Indian medical jurisprudence and certainly more than the contract law requirement.

a sufficiently accessible fashion, in accordance with accepted industry standards, and on this basis secure user consent, they could act against user interest (subject to the data protection authority itself not barring any specific practice under Section 33, on grounds that it is likely to lead to harm to the data principal). To illustrate, consider two situations:

- In the first situation, sufficient details and information about data processing practices are provided by a data fiduciary in its privacy policy. A user however doesn't read the same but nevertheless consents to the processing (say by ticking a check box). At a later point of time, the user objects to certain forms of processing arguing that these go against his or her interests.

- In the second situation, vague or unclear information is provided by the data fiduciary in its privacy policy. The user nevertheless reads the information provided, reaches a conclusion as to its meaning and on this basis consents to processing. At a later point of time, the user discovers that his or her personal data is being processed in a manner that does not accord with his or her understanding of the given disclosures.

In the first situation above, the data fiduciary would have to show not just that it had provided sufficient information to enable the user to assess the material risks and effects of the processing, but also that this was provided in a manner that enabled easy access and understanding of the terms. Should this be done in an adequate and reasonable manner, the data fiduciary would not be liable to the user.

On the other hand, in the second situation, the data fiduciary would be liable for not having provided sufficient disclosures to the user or not having provided the information in a manner in which it was easily understandable. As mentioned previously, the onus would be on the data fiduciary to show that it took reasonable steps to provide relevant information to the user and was acting in a bona fide manner. Given the good faith requirements under the law (and in a fiduciary relationship more generally), the data fiduciary will not be able to use ambiguities in the language of privacy policies to disadvantage the user.

4.2.4. Grounds for non-consensual processing

In addition to the ground of consent described previously, Sections 13 to 17 list various additional grounds that can be taken to lawfully process personal data.[115]

The standard of care expected of data fiduciaries who rely on the "reasonable purposes" ground for processing does not appear to impose a "fiduciary" standard on data fiduciaries.[116] The provision seeks to balance the interests of the data fiduciary with that of the data principal and does not per se give the data principal's interests and expectations primacy.

4.2.5. Limiting data collection and storage

Data fiduciaries are obliged to only collect data that is necessary for the specified and other compatible purposes and no more.[117] Data fiduciaries can only retain data for as long as it is "reasonably necessary" to fulfill the purposes for which it has been collected.[118] Obligations of the data fiduciary would continue to apply as long as the data has not been deleted or anonymised.

These provisions could be said to ensure that data fiduciaries only process data in accordance with the needs and expectations of the data principal. Once the declared purpose of processing has been met, the data must be deleted - thereby ensuring that the possibility of abuse of the data principal's information is reduced.

The above provisions are further added to by inclusion of a 'right to forget' using which the data principal can seek to prevent continued disclosure of personal data in certain circumstances.[119]

115 These include processing required: (a) to perform functions of the state, (b) to comply with orders of adjudicatory authorities, (c) for prompt action, (d) for purposes of employment, and, (e) processing for reasonable purposes.

116 This provision can be invoked should processing be considered necessary to meet a "reasonable purpose" which is to be determined based on factors such as (a) the interest of the *data fiduciary* in processing, (b) whether it is reasonable for the data fiduciary to obtain consent, (c) any public interest in the processing, (d) the effect of the processing activity on the rights of the data principal, and, (e) the reasonable expectations of the data principal with regard to the context of the processing. The proposed data protection authority is required to notify purposes that can be considered "reasonable" taking into account the above factors.

117 Section 6 of the draft PDP Bill.

118 Section 10, draft PDP Bill.

119 Section 27, draft PDP Bill.

4.2.6. Transparency and accountability

The PDP Bill contains a number of provisions that aim to enhance the transparency and accountability of the data fiduciary towards the data principal. This is done by ensuring adequate notice to the data principal, conferring access and modification rights, ensuring that the personal data is kept up to data and accurate, providing for data audits, and importantly, providing for data breach notification.

Importantly, the law recognises:

1. an obligation on the data fiduciary to provide notice to the data principal (no later than the time of collection of data or in cases of indirect collection, as soon as reasonably practicable);[120]
2. a general obligation on data fiduciaries to make certain basic information regarding the scope of processing easily accessible;[121]
3. an obligation on the data fiduciary to take reasonable steps to ensure any personal data being used to make decisions about an individual is up-to-date and accurate and to inform third parties with whom data is shared about any inaccuracies in the personal data;[122]
4. rights of the data principal to access and modify personal data;[123] and
5. rights to seek explanations of the processing being undertaken.[124]
6. requirement for data audits,[125] and assignment of data trust scores (for significant data fiduciaries).

The PDP Bill does recognise the need for data breach notification - though in this regard, the data fiduciary is only mandated to inform the proposed Data Protection

120 The Bill lays out various requirements of such a notice in Section 8, which includes for example the need for the data fiduciary to provide details of the categories of data being collected, the purpose of collection, contact details of the data fiduciary, procedure for grievance redress, time of retention of data, data trust scores, etc.
121 Section 30, draft PDP Bill.
122 Section 9, draft PDP Bill.
123 Section 24, draft PDP Bill.
124 Section 25, draft PDP Bill.
125 Section 35 of the PDP Bill requires data fiduciaries to have its policies and practices audited by an independant data auditor, who is required to evaluate compliance with the obligations under the law.

Authority (the "DPA") of the same (and that too only in cases where defined harms are likely to arise as a result of the breach).[126]

An interesting possibility given the fiduciary duties placed on doctors to expose dishonest or unethical conduct of other professionals, is a requirement for data fiduciaries to be required to inform the data principal or data protection authority of any third party data breaches or discovery of harmful/unethical practice being committed by another entity. The law could alternatively ensure adequate whistleblowing protections to encourage disclosure of practices that go against user interest.[127]

Overall the PDP Bill does indeed put in place significant duties aimed at reducing information asymmetry. However, the design of the data breach provision detracts from the fiduciary nature of relationship. Not only is the reporting requirement linked to the fiduciary recognising the possibility of harm to the data principal,[128] this provision denies the data principal an opportunity to make an informed choice on whether to continue to repose trust and confidence in the fiduciary and reduces their autonomy (Bailey, Parsheera, Rahman, and Bhandari 2018).[129]

4.2.7. Standards of care

The PDP Bill seeks to ensure that data fiduciaries process personal data in a manner proportionate to the risk involved. The requirement of "reasonable" processing under Section 4 in particular imposes an objective standard of care on data fiduciaries, that is as expected in fiduciary relationships.

126 The DPA can choose to have the data fiduciary inform the data principal of the breach, based on the severity of harm that may accrue or in case any ameliorative measures need to be adopted by the data principal.

127 The criminalisation of white hat hacking in the law also limits the ability of user's to know about harmful data processing practices.

128 This sets a standard which may lead to confusion and inadequate protection as it may be possible for a data fiduciary to deny reporting a data breach on the grounds that they assumed it would not cause harm (Bailey, Parsheera, Rahman, and Bhandari 2018).

129 It is also strange that while the PDP Bill is largely based on the concept of valid consent - which is typically based on having access to all material information, it denies users the ability to always know about the data breaches that may have occurred. Presumably, the law takes such a position to avoid excessive obligations and costs on data processing entities as well as to protect against instances of public panic.

The law also attempts to implement a system whereby data fiduciaries can demonstrate their compliance with the obligation of "fair and reasonable" processing without waiting for the data principal to ex-post identify non-compliance. This takes the form of obligations such as:

- building in appropriate security safeguards including relevant access controls that are proportionate to the nature, scope and purposes of processing, risks involved and likelihood and severity of harm;[130]
- privacy by design implementation, which notably requires the data principal's "interests" to be considered at all stages of the processing;[131]
- the obligation to ensure that entities engaged in downstream processing are also subject to relevant data confidentiality and security related obligations[132] and,
- providing notice (to users, regarding data breach, etc.) at appropriate times, permitting the user to exercise rights provided by the PDP Bill.

The duty to ensure data protections run with the data is particularly important. Undisclosed and unchecked downstream uses of data are a significant source of privacy harm for individuals. Further, the requirement to ensure data principal interests are considered while designing and implementing processing systems is also noteworthy.

The PDP Bill therefore seeks to implement measures to not just punish parties post-breach, but actively encourages institution of measures that could prevent harms from arising in the first place. This appears to fit well with the fiduciary concept in that the law seeks to be preventive in nature rather than curative.

4.2.8. Additional obligations

The draft Bill casts certain additional obligations on three specific types of data fiduciaries who are seen as posing enhanced risks to individuals due to the additional imbalances presumed in the nature of the relationship between the parties.

130 Section 31, draft PDP Bill.
131 Section 29, draft PDP Bill.
132 Section 37, draft PDP Bill.

These categories include fiduciaries that process personal data of children, a subset of this category that are notified as "guardian data fiduciaries" and separately, "significant data fiduciaries".

Given the limited understanding that children have for the consequences of their actions, the draft Bill seeks to ensure additional protection to those under eighteen years of age, by mandating that their data be processed only in a manner that "protects and advances" their "rights and best interests".[133] The DPA is also empowered to notify a special class of "guardian data fiduciaries" who are barred from profiling, tracking, behavioural monitoring, directing targeted advertisement at children or otherwise carrying out any processing that may cause "significant harm" to the child.

The DPA may also notify entities as "significant data fiduciaries"[134] who may be subject to certain additional obligations such as submitting privacy impact assessments,[135] record keeping requirements,[136] data audit requirements,[137] and the need to appoint a data protection officer.[138]

These enhanced duties are parallel those expected in typical fiduciary relationships - where greater duties are cast on entities in more unequal relationships.

4.2.9. Remedies

The PDP Bill lays out a series of remedies that can be used by a data principal against data fiduciaries and processors. These are far broader and more strict than envisaged by

Balkin, and in certain circumstances, go well beyond the two American laws referred to previously by criminalising various types of behaviour.

133 All data fiduciaries processing a child's personal data are required to implement mechanisms for age verification and parental consent.

134 Per Section 38 of the draft PDP Bill, the decision to classify an entity as a significant data fiduciary should have regard to factors such as the volume of data processed, the sensitivity of the data, the risks of harms that may occur due to the processing, and other relevant factors.

135 Section 33, draft PDP Bill.

136 Section 34, draft PDP Bill.

137 Section 35, draft PDP Bill.

138 Section 36, draft PDP Bill.

Data principals can seek remedies in case of breach of any of the obligations contained in the law, or in case harm results from such a breach.[139] This provision therefore is similar to that in fiduciary relationships, as mere breach of duty can confer a cause of action. However, the first port of call for a aggrieved data principal is the data fiduciary which is required to establish a grievance redress mechanism. The complaint can then be escalated to an adjudicatory authority.[140] The jurisdiction of civil courts is specifically excluded by the statute.

The Bill does not cap the amount of compensation payable. The maximum fine/penalty payable under the law is INR fifteen crore or four percent of global turnover, whichever is higher. This amount is fairly substantial and in ordinary cases could be seen as constituting a significant deterrent against breach, which would be in keeping with the fiduciary concept. However, one may question whether four percent of turnover is a sufficient deterrent to some of the bigger digital conglomerates, who despite having been fined large sums of money in the US and the European Union have not always significantly improved their privacy practices.[141]

The PDP Bill also empowers the data protection authority with a range of powers which it enable it to *inter alia* scrutinise data processing practices, and if necessary bar or modify any practices that may lead to harm to data principals.[142] Interestingly, the PDP Bill empowers data protection authorities to carry out suo moto inquiries on suspicion that fiduciaries are engaging in acts "detrimental to the interests of data principles".[143] This provision does appear to place a high standard of compliance on data fiduciaries - similar to the American laws discused previously. It is however

139 The term "harm" is defined in Section 2(21) as including (i) bodily or mental injury, (ii) loss, distortion or theft of identity, (iii) financial loss or loss of property, (iv) loss of reputation or humiliation, (v) loss of employment, (vi) any discriminatory treatment, (vii) any subjection to blackmail or extortion, (viii) any denial or withdrawal of a service, benefit or a good resulting from an evaluative decision about the data principal, (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out a fear of being observed or surveilled, or, (x) any observation or surveillance that is not reasonably expected by the data principal.

140 Appeals lie to an Appellate Tribunal and then the Supreme Court of India.

141 Tech majors such as Google and Facebook have in fact faced fines in the billions of dollars, though the impact of these has been questioned. Refer for instance to (Tiku 2019), (Patel 2019) and (Vaidhyanathan 2019).

142 Refer Section 33(5) of the PDP Bill.

143 Refer Section 64(1)(a). The Authority has a wide range of powers in such situations including an omnibus 'do anything I tell you to' clause in Section 65(h).

interesting that such a standard is not found consistently through the law (notably it is absent from Section 4). The law appears therefore to permit the power of inquiry in greater situations than it punishes.[144]

4.2.10. Overall analysis of duties under the PDP Bill

Similar to the obligations imposed in traditional fiduciary relationships, the mechanisms used by the PDP Bill to address the agency problem can be summarised under five broad heads as below:

- *Limitations on the authority/ability of the data fiduciary to act without knowledge of the data principal:* Provisions pertaining to purpose limitation, limitations on data collection and storage, informed consent as the primary ground for processing data, right to correct data, etc.
- *Duty of loyalty and care:* Requirement for fair and reasonable processing, obligations to secure data and implement privacy by design measures, requirement to ensure obligations flow with the data, etc.
- *Reduction of information asymmetry:* Provisions pertaining to notice, high standards of consent, right to access and correct data, transparency (record keeping and disclosure) and accountability related provisions such as requirement to provide various types of information pertaining to the processing to the data principal, conduct data audits, have a data trust score for certain entities, requirement of data breach notification, etc.
- *Standard of care:* A reasonable and proportionate standard of care is required by the PDP Bill. Obligations are scaled based on the risks of any particular processing practice, as well as the type of personal data concerned and the nature of entities involved. Notably, greater obligations are imposed on significant data fiduciaries and guardian data fiduciaries.

144 This could be seen as being in the interests of data principals - in that the the authority is given greater power to act practices that may be dodgy or may be pushing the limits of acceptability. However, it could also lead to rent-seeking behaviour by permitting inquiries into situations that are permitted by the law but are not always favourable to the data principal (for instance, in the case of behavioural advertising, contextual pricing, etc.).

- *Remedies:* Data principals can approach the data fiduciary and then adjudicatory forums for breach of the duties cast on data fiduciaries by the law. Mere breach of the obligations under the law can lead to penal action. The penalties that the draft law imposes are fairly stringent, with a maximum penalty being 4 percent of worlwide turnover of the violating entity.

Overall, it can be seen that the PDP Bill does indeed implement duties akin to that in traditional fiduciary relationships. The duties discussed above do try and ensure that the data fiduciary processes data in accordance with expectations of the data principal / that the data principal is aware of the processing taking place and its effects i.e. that the agency problem in the relationship is reduced.

However, the scope of some of these duties and the standard set by them are not as high as seen in cases of traditional fiduciary relationships (particularly those of a doctor-patient and a trustee-beneficiary). The general lack of a requirement to act in the data principal's interests or to his/her benefit are particularly notable. This also reflects in the standard of some of the additional duties.[145]

The fundamental tenet of fiduciary relationships is the duty of loyalty, which requires the fiduciary to give primacy to the beneficiary's interests. This is also reflected in the various disclosures that the fiduciary is required to make if he engages in conduct that may apparently be considered prejudicial to the beneficiary's interests. The PDP Bill is based on a notice consent framework that seeks to safeguard data principal's interests not by requiring processors to place their interests over that of the data fiduciary, but only by ensuring that the data principal know what it is they are consenting to. The underlying requirement of the PDP Bill is that there is that processing should be as per the "reasonable expectation" of the data principal, rather than in its interest.

One may however question whether such a standard is appropriate in the privacy context, given the extent of vulnerability in many relationships of information exchange particularly in the digital ecosystem. The difficulty for individuals in

145 For instance, trust law, company law and medical law impose greater restrictions on the profit earning capacity of fiduciaries than the PDP Bill does.

comprehending privacy risks, even when complete disclosures are made, may in fact mean that a standard closer to that used in trustee-beneficiary relationships may have been more suitable.[146]

That said, data processing practices that are particularly risky could be barred by the data protection authority. While this could protect users against particularly dangerous processing activities, the standard is still not the same as requiring the data fiduciary to act in the interests of or for the benefit of the data principal. Further, empowering the authority in this manner appears to detract from the fiduciary concept in that it enables ex-ante decision making by an executive authority, rather than enabling practices to be adjudicated as being in consonance with (or in breach of) fiduciary obligations by an adjudicatory authority. The PDP Bill therefore casts a considerable responsibility on the data protection authority to act transparently, in a nuanced manner, and to adequately consider all interests in drafting its regulations.

4.3. Does the PDP Bill contain any novel data protection obligations?

As described above, the PDP Bill primarily utilises a notice and consent based model to protect user privacy (though this is enhanced and has various safeguards that are not normally present in contract law). The law implements a high standard of consent and limits the ability of data processing entities to act outside the bounds of what user's consent to. The consent related provisions are buttressed *inter alia* through provisions that aim to reduce the information asymmetry in the relationship and that require the data processing entity to implement various security safeguards, etc.

However, the duties of loyalty and care that could be imposed using the fiduciary concept are not fully exploited. The duty of loyalty imposed under the PDP Bill is not particularly strong as say, the case with the two draft US laws. The PDP Bill esentially

146 The trustee-beneficiary relationship casts a greater duty of loyalty on the trustee (than company law) as in many cases the beneficiary will not be capable of properly assessing risks at all. This may occur for instance, where the beneficiary is a minor. Merely securing consent would be insufficient to allow the trustee to act against the beneficiaries interests in such cases.

allows users to consent to various processing activities that may not always be in their interests - subject to proper consent.

It becomes relevant then to try and compare the obligations imposed under the PDP Bill with data protection frameworks that do not use the fiduciary concept. Is the PDP Bill essentially similar to laws such as the GDPR, or does it add anything novel?

We provide a brief overview of the obligations imposed under the two laws in Annexure - II to this paper.

A summary comparison of the two laws reflects little difference in the range of obligations imposed (though the exact scope/contours of the obligations are different based on the specific language used in the laws).

For instance, there is little difference in the scope/coverage of the laws, the general principles of processing, the grounds for processing,[147] the requirement for processing to be fair and informed, the nature of consent, additional protections to specially sensitive data,[148] the provisions pertaining to reduction of information asymmetry including by way of notice requirements, information on processing, etc. Two differences pertaining to information related provisions do stand out:

- certain provisions such as that of a data protection impact assessment, carrying out data audits, additional record keeping requirements, and appointment of data protection officers only apply to significant data fiduciaries or other notified data fiduciaries under the PDP Bill;
- The certification mechanisms specified in the GDPR are voluntary, and must be proportionate (i.e. different for small, medium, large businesses). The use of trust

147 Three differences stand out in so far as the grounds for non-consensual processing are concerned. First, the GDPR recognises performance of a contract as a ground for processing while the Indian law does not; second, the Indian law empowers the data protection authority to notify certain "reasonable practices" instead of the GDPR's "legitimate interest" ground; and third, the PDP Bill recognises processes related to employment as a specific ground for processing. The GDPR does not and instead empowers member states to implement additional safeguards in such contexts.

148 The GDPR contains a general prohibition of processing such data, with a list of 10 exceptions. The PDP Bill does not contain a general prohibition but only permits processing of such data on 3 grounds. The PDP Bill specifies more categories of personal data as sensitive than the GDPR does.

scores / ratings and data audits in the PDP Bill is mandatory for significant data fiduciaries or those otherwise notified to do so by the data protection authority.

However, in some cases the protections offered by the PDP Bill are lesser in scope than the GDPR. This is notable for instance in terms of the right to forget / right to erasure, the right to object to processing and right against automated individual decision making. On the other hand, the PDP Bill does appear to put in place higher obligations when it comes to the processing of children's data by using a "best interests" framing and by barring various harmful practices altogether.

The two laws also differ in:

- Scope of cross border data transfer related provisions: By mandating compulsary localisation of certain categories of sensitive personal data, the PDP Bill restricts the autonomy of parties when compared to the GDPR. This detracts from the fiduciary concept which would enable a fact specific, benefit or interest based determination of whether a particular transfer would be permitted.[149]

- The nature of liability: The GDPR permits penalties to be imposed for breach of the law, while compensation is payable for material and non-material damages. The terms are left undefined. The PDP Bill permits penalties to be imposed for breach of the law or causing certain defined harms. Compensation too, is linked to the defined harms. A higher standard of significant harm is used to trigger additional obligations on data fiduciaries.

- Remedies: The GDPR envisages complaints being handled by the supervisory authority or courts. The role of the data controller itself is limited, though the internal data protection officer may indeed take/resolve complaints. The PDP Bill excludes the jurisdiction of civil courts and lays down details of a grievance redressal process at the level of the data fiduciary. Complaints are also handled by the adjudicatory mechanism established under the draft law.

149 In some situations, cross border data transfers of even sensitive data may be in the interest of the data subject. For instance, where transfer of sensitive personal data may help in terms of fraud prevention in the use of payment services, where the data may be stored more safely or at cheaper rates, etc (Bailey and Parsheera 2018).

The role played by the supervisory authorities in the two laws are largely similar. Both laws envisage fairly interventionist roles for the regulatory authority, and cast them in a paternalistic role. The regulatory agencies have extensive powers of investigation and inquiry, validating processing practices, enforcing compliance, etc., though in some respects the PDP Bill casts a greater onus on the Indian regulator. For instance, the Indian authority is required to decide if data principal's should be notified of data breach and is responsible for preparing codes of practice and various forms. It also has the power to notify "reasonable practices" under Section 17, "significant data fiduciaries", additional categories of sensitive personal data, etc.

4.4. Effect of using the data fiduciary framing in the PDP Bill

So what is the overall effect of the fiduciary framing in the PDP Bill and is this really required to justify the obligations imposed by the PDP Bill?

As is evident from the previous discussion, the use of the term "data fiduciary" in the draft law does not in itself imply imply that the high standards that come with fiduciary obligations will necessarily be imposed on all data processing entities. The definitions section in the PDP Bill is not a deeming provision. Whether or not data processing entities are fiduciaries (in general) will continue to be a matter of fact. If based on the circumstances at hand, the parties are in an actual fiduciary relationship, it is possible for relevant standards over and above those in the PDP Bill to be imposed.

However, the entities that come within the definition in the law would be subject only to the (fiduciary like) obligations provided in the PDP Bill itself. Users could therefore access these obligations without having to "prove" a fiduciary relationship in every case - they would just have to show that the entity was acting within the scope of the definition provided (i.e. a party who determines the purposes and means of processing).

To illustrate, a user will still be able to succeed in a claim against a digital platform under section 88 of the Trusts Act after having shown on facts that the relationship is

fiduciary in nature.[150] A court could, in such circumstances, require the fiduciary to adhere to duties of loyalty and care that more closely correspond with those imposed on traditional fiduciaries.

The use of the phrase "data fiduciary" is largely meaningless from a purely legal perspective. What it does achieve is in terms of its symbolic and signalling value to courts, the general public and businesses.

One may speculate that this could be an important reason in choosing to use the fiduciary concept in the draft law. It is not impossible to imagine that the PDP Bill uses the fiduciary concept to cast the illusion of crafting a new, user-centric privacy framework, without actually changing too much from notice and consent based regimes (which have been criticised as being inadequate in the digital ecosystem and in particular in a country such as India).[151] The fiduciary concept is something that is used in many legal contexts and is a term that people are familiar with (even if the nuances of this relationship are not very well understood). Doctors, guardians and other such fiduciaries are commonly expected to act in their beneficiary's interests / display a high standard of loyalty towards them. Use of the phrase "data fiduciary" may well lead people to assume or expect that the PDP Bill also imposes such a high standard of loyalty on data processing entities. Use of the terminology could therefore make the Bill more palatable to civil society which craves greater standards of rights protection, thereby making it easier to "sell" the legislation to the general public amongst other stakeholders.[152]

In this respect its also interesting to note that the Committee did not really consider many alternatives to using the fiduciary concept i.e. whether the same end-results could be achieved through other means or indeed whether using the fiduciary concept confers any specific benefits over other typical models of data protection. For instance, there is no consideration of whether the use of this concept is preferable to

150 It would not be open to merely point at the PDP Bill as a deeming provision in this respect.

151 In this context, the differences between the reasoning used by the Committee and the actual content of the law are also notable. As indicated previously, while the Committee consistently uses a "best interests" framing to describe the relationship between data fiduciaries and principals, this phrase is conspicuous in its absence from most of the PDP Bill.

152 Khan and Pozen make a similar argument when they point to how the low standards of care suggested by Balkin are one of the reasons the information fiduciary framing has received backing of commercial interests in the US.

basing data protection obligations on the need to mitigate certain specific types of harms. The only other framework apparently considered by the Committee is that of using a property based framework, which would confer ownership rights over personal data to the individual concerned. This model was overlooked on grounds of being "philosophically flawed, legally counter-productive, and practically unimplementable" (Sengupta 2018).

While there is undoubted merit in rejecting an ownership based model for protection of personal data, it is unclear why this *ipso facto* requires adoption of a fiduciary based model. Notably, the GDPR does not adopt either, but at the same time attempts to empower individuals and give them control over how their data is used.[153] The motivation for using the fiduciary concept could therefore well be the need to differentiate the PDP Bill from laws such as the GDPR, particularly in view of the Committee's self-imposed mandate to find a "fourth path" to data protection i.e. one that is different from the privacy frameworks used in Europe, the US and China.

Ultimately, there does not appear to be any particular reason for the use of the fiduciary concept in the PDP Bill. It confers no real novel benefits to users (as is the case with the two draft US laws). The draft PDP Bill largely replicates the (high) notice and consent standards together with other information asymmetry reducing provisions found in the GDPR, which does not use the fiduciary concept. The use of the fiduciary framing therefore appears largely cosmetic.

The draft PDP Bill could, instead of using the fiduciary concept, achieve more or less similar results by basing its obligations on the risks of harm that could arise in various contexts. This is already done to some extent in the draft law - notably by permitting the data protection authority to bar practices that lead to certain defined types of harm. Such a method, whereby the law proscribes certain effects (or specific uses of personal data) can create a uniform standard of rights protection, while ensuring certainty in so far as businesses are concerned. It could however limit innovation and

153 The GDPR uses a strengthened notice and consent based framework, together with certain minimum standards of behaviour that have to be respected by all data processing entities. As described previously, the broad structure of the obligations imposed under the GDPR and PDP Bill is exceedingly similar.

cast a significant regulatory burden on the data protection authority. This may not be ideal given problems with state capacity and the limited privacy awareness and jurisprudence in India.[154]

5. Conclusion

The information fiduciary concept is an interesting method developed by Jack Balkin to justify regulation of privacy harming practices in the US constitutional scheme. The application of the fiduciary concept to the data protection context *prima facie* appears a feasible way to protect user rights due to the duties of care and loyalty expected of fiduciaries. However, the concept also suffers from certain infirmities. For instance, all data processing entities may not be in fiduciary relationships with individuals. Further, the fiduciary concept may not be ideal for the framing of a general data protection law given that it seeks to protect and therefore privilege the beneficiary's interests over that of the principal. This may not always be desirable in a data protection context (where balancing of interests may be required).

The PDP Bill borrows Balkin's concept of information fiduciaries and tailors this to the Indian context in light of Indian public interest requirements and a standard of care thought appropriate to the digital ecosystem (the adequacy of which is however, subject to debate).

Due to the focus on balancing business and data protection interests, the PDP Bill does not confer as high a standard of loyalty and care as may be normally expected in a fiduciary relationship (and in this respect, departs from the discussion in the Report of the JSK Committee). The PDP Bill adopts the low standards of loyalty and care prescribed by Balkin. Unlike the law in the case of doctors, company directors, and particularly trusts, there is no general requirement for fiduciaries to act in the beneficiary's interest or to their benefit (except in the context of children).

154 The data protection authority's ability to bar certain data processing practices is substantially different from the law barring practices in view of their breaching fiduciary principles. In the former case, it will be the executive authority deciding on what practices to bar, while in the latter case, it will be adjudicatory authorities doing so.

Data processing entities will be required to comply with standards of good faith and reasonableness that are akin to the "fair dealing" standards found in contract law in many jurisdictions. This standard is higher than that under current Indian contract and consumer protection law, but is similar to requirements in the insurance industry. Fiduciaries will have to make all material disclosures, and act in accordance with generally accepted industry standards. Practices such as targeted advertising, tracking, etc., will not per se be barred except where children are involved (or where the data protection authority believes that such practices are likely to harm individuals and therefore bar them). The powers granted to the data protection authority to bar certain practices, while possibly useful given the low standards of loyalty and care cast on fiduciaries, also implies that decisions regarding permitted practices will be made by executive authorities rather than adjudicatory authorities.

But the Bill does, to an extent, meet the aim of preserving autonomy i.e. decision making power of individuals, and reducing inequality in bargaining power. This is primarily done by subjecting data processing entities to strict consent related requirements including by specifying (high) standards for notice and ensuring that consent must be granular. The provisions related to information disclosure, limited data collection, deletion, purpose limitation, data audits and privacy impact assessments, etc., are also vital in reducing the agency problem in the relationship.

That said, the PDP Bill does confer somewhat less autonomy to individuals than what the full use of the fiduciary concept may entail.[155] When compared to Balkin's concept, one sees that the Bill does envisage broader rights and more effective remedies. However, the lack of a proper data breach notification clause is a significant difference. In addition to the absence of a general duty of loyalty under the PDP Bill, the law also avoids casting obligations on entities processing non-personal data, even if this belongs to an individual. The law therefore does not circumscribe the use of derived data (except where this can be used to identify an individual). The PDP Bill therefore does not utilise the fiduciary concept to its fullest extent.

155 The limited data breach notification requirement and the large scope of (ex ante) powers given to the data protection authority are significant in this regard.

Overall, there appears no real need for the PDP Bill to utilise the fiduciary concept. The same range of obligations could be imposed by statute without reference to this concept, as is done in the case of the European GDPR. One may speculate that this is the case either to differentiate the PDP Bill from the GDPR, or taking a more uncharitable view, to make it appear that the law contains a higher standard of rights protection than it actually does.

6. Annexure - I: Fiduciary Relationships in Indian Law

The law, first through tort and increasingly through statute, has recognised the concept of fiduciary relationships in an expanding number of contexts.[156] We now examine how fiduciary relationships have been recognised in Indian law by analysing fiduciary duties in the context of a trustee-beneficiary, director-company and doctor-patient relationship.

We do not attempt to list all the duties that the law may impose in any of these contexts, focusing instead on illustrating the key methods used by the law to overcome the vulnerabilities in each type of relationship. Specifically, our attention is on the duties placed on fiduciaries that govern their authority to act on behalf of the beneficiary, the scope of the duty of loyalty, the mandated standard of care, the methods of reducing information asymmetry, the fiduciary's confidentiality requirements, and the remedies made available to the beneficiary in each of these relationships.

6.1. Trusts

Historically, trusts developed to enable a landowner (settlor) to transfer property to a third party (trustee), to hold and deliver for a beneficiary, who was not normally qualified to hold title (say due to being a minor) (Wynen 1949) and (Ames 1908).

156 Some of the most common include trustees, agents, administrators, corporate directors, lawyers, and investment advisors.

The trustee would be the legal owner of the property, but was bound in equity to hold it for the beneficiary.[157]

The Indian Trusts Act, 1882, (Trusts Act) defines a trust as an obligation annexed to the ownership of property that arises out of confidence, reposed and accepted or declared and accepted, in the owner, for the benefit of another.[158]

The vesting of title in property with a trustee is at the core of a trust relationship. The power created by such a right is ameliorated by law imposing rigorous duties on trustees - the most essential of which is the requirement for trustees to act in good faith, for the beneficiary's interest in preference to the trustee's own interests (Clarry 2014). Trustees are not even usually entitled to recieve payments for their services - trusteeship is not an office of profit.[159]

A trustee has two primary roles to perform - a distributive role, per which they must ensure that the gains arising out of the trust property are distributed to the appropriate beneficiaries as per the terms of the trust and expectations of the settlor (Hay's Settlement Trusts, Re 1981), and a managerial role, which is concerned with safeguarding and developing the value of the trust property (Mitchell 2010). In order to perform these functions, the law prescribes a number of duties, which we examine below:

- **Limitation of authority:** Section 11 of the Trusts Act requires trustees to fulfill the purposes of the trust, and to obey the instructions of its settlor, except as modified by consent of the beneficiaries (who must be competent to contract).

157 Trusts therefore became recognised in the law due to the imperfect ability of the both the settlor and the beneficiary to adequately monitor the behaviour of a trustee. The trustee, being the legal owner of the property had absolute power to deal with it. In modern trusts, the same agency problem persists. (Leslie 2005).

158 Section 3, Indian Trusts Act, 1882. The essential features of a trust include:

- The obligation must relate exclusively to property. The ownership of the property should vest in the trustee.
- The obligation must arise out of confidence which the author of the trust reposes in the trustee, such obligation being accepted by the trustee.
- There must be an obligation to use the property for the benefit of a third person (beneficiary).

159 Section 50 of the Trusts Act recognises that a trustee cannot expect payment for services rendered by default i.e. he or she is entitled to renumeration only when the same is specifically granted in the trust instrument, by order of court or by contract with the beneficiary. Trusts therefore differ from certain other fiduciary relationships where remuneration is accepted as part of the service.

As a general rule, trustees cannot deviate from the trust deed, even if by doing so he or she would be acting in the interest of the beneficiaries.

The power of modification rests only with the beneficiaries. Beneficiaries can also manage their relationship with trustees by renouncing their interest in the trust, by transferring the beneficial interest in the trust to another party, or by extinguishing the trust.[160] They can also seek to discharge a trustee under Section 71.

Trustees can themselves only renounce their duties subject to consent of the beneficiary, an express provision in the trust deed or upon securing authorisation from a court.[161]

- **Duty of loyalty / No conflict:** The two main duties of a trustee comprise a prohibition on self-dealing[162] and a requirement of fair-dealing.[163]

  These rules are captured in various provisions of the Trusts Act such as Section 52, Section 53 and Section 88.

  Per Section 52, a trustee cannot, directly or indirectly, purchase trust property intended for sale, on his or her own account or as an agent for a third party. The law does not go into the question of whether the transaction is beneficial or not but just assumes fraud in such cases (Swaminatha Aiyar v. Jumbukeswaraswami 1930) and (Morse v. Royal 1806).[164]

  Section 53 permits a trustee to purchase the interest of a beneficiary only subsequent to court permission, which will only be given when the court is satisfied that the transaction is manifestly for the advantage of the beneficiary.

160 Section 78 of the Trusts Act recognises that while normally only the settlor of the trust can revoke it, the beneficiary may do so when capable of consent.

161 Section 46, Trusts Act.

162 Under the self-dealing rule, the trustee is not allowed to sell trust property to himself. In case he sells to himself, the transaction is rendered voidable at the option of the beneficiary, regardless of how fair the transaction is.

163 Under the fair-dealing rule, the transaction can be set aside by the beneficiary unless the trustee can show that he has taken no advantage of his position and has made full and material disclosures to the beneficiary, and that the transaction is fair and honest.

164 In order to prevent any possibility of self-dealing, the law presumes invalidity of certain acts, not because there is fraud, but just because of the possibility that there may be fraud (Langbein 2005).

Section 88 prohibits the trustee (or any other party in a fiduciary relationship) from using their fiduciary position to gain a pecuniary advantage or placing themselves in a situation where they may profit from a conflict of interest. Any such profit made, is held for the beneficiary.

- **Standard of care:** Section 15 of the Trusts Act provides that a trustee should deal with the trust property as carefully as a man of ordinary prudence would deal with such property if it were his own.[165] Some cases have held this to be a standard of rendering "every possible advantage to the beneficiaries" (Fatima Fauzia and Ors. v. Syed Ul-Mulk and Ors. 1979).

  A failure to act reasonably and with due care and good faith renders the trustee liable for the loss, destruction or deterioration of the trust property.[166]

  Section 49 also enables courts to step in and exercise a trustee's power, should he or she be failing adhere to the duties to act reasonably and in good faith.[167]

  The interests of the beneficiary are also protected by providing that the trustee cannot delegate his or her functions (unless specifically permitted by statute).[168]

  This ensures that the trust is administered as per the competence the settlor expected from the trustee, towards protecting the interests of the beneficiaries and the trust property.[169]

- **Reducing information asymmetry:** Section 19 of the Act requires the trustee to keep clear and accurate accounts of the trust property. The trustee is liable to

165 There are many provisions in the Trust Act that embody the above standard. Notably, Section 13 requires the trustee to take all reasonable steps to protect the trust property, Section 16 permits the conversion of perishable trust property so as to ensure the benefit of the beneficiary, Section 18 permits the trustee to take measures to prevent acts destructive or injurious to the trust property, even against a beneficiary, where the trust is made for the benefit of several persons in succession.

166 The term "good faith", requires a person to act with "due care and attention expected a man of ordinary prudence." (Fatima Fauzia and Ors. v. Syed Ul-Mulk and Ors. 1979).

167 Under Section 61 of the Trusts Act, beneficiaries can also compel any act of duty or restrain the trustee from acting in probable breach of trust.

168 Section 47 of the Trusts Act permits delegation where provided in the trust deed, it occurs in the regular course of business, it is necessary, or is done subsequent to consent of the beneficiary (who must be competent to contract).

169 Since the office of the trustee is founded on the relation of personal confidence, delegation defeats the purpose (Turner v. Corney 1841). The executors of a trust also cannot confer power upon strangers that the testator alone had the power to confer. For example, when the trustees were granted powers to appoint their own successors, they could cannot exercise that power in a way to appoint new trustees (Dinshaw Maneckji Petit v. Jamsetji Jeejeebhoy 1909).

render accounts in the discharge of his or her duty to manage the trust property, and for the purpose is required to maintain its account separately.[170] A failure to maintain accounts and provide evidence thereof, can on its own impose liability, even if the trust was being properly administered (Payne v. Evans 1874).

Apart from maintenance of accounts, Section 57 of the Trusts Act requires the the trustee to furnish full and accurate information to the beneficiary as regards the amount and state of trust property. The beneficiary has a right to inspect and take copies of the accounts of trust property.

- **Remedies:** Breach of duties owed to a trustee or breach of trust, imposes an obligation on the fiduciary to restore the loss caused to the beneficiary. Indian law departs from the English law to the extent that where English courts have the power of relieving honest trustees from their liability for breach of trust, Indian courts have been given no power to protect trustees in any case where a clear breach of trust has been committed. This is because Indian law treats breach of trust an evil in itself. Liability cannot be absolved by arguing that the breach of trust was beneficial to the trust (Mariyam Biwi v. Natharsa Rowther 1978).

Damages aside, the Trusts Act also recognises remedies in the form of injunctions, and recognises that illegal gains are to be held for the beneficiary. Beneficiaries can trace property where there is an identifiable conversion by the trustee acting in breach.[171]

6.2. Company directors

The primary executive agents for a company are its directors - officers of the company, appointed by virtue of their expertise and professional skills, to manage and run the affairs of the company. They therefore have significant power over the affairs and

170 In case the trustee mixes trust funds, the trustee has the burden of proving that a particular property is his private property and not the trust property (Narayan Bhagwantrao v. Gopal 1960).

171 Section 63 of the Trusts Act permits the beneficiary to sue a third party who has received trust property in a manner inconsistent with the trust, for a declaration of the beneficiary's title to the property and for restitution. Section 64 however limits the above right in cases where the transferee acted in good faith and without knowledge of the trust.

functioning of a company.[172] In order to protect the interests of investors as well as that of the general public, the law recognises a series of duties and obligations of directors which aim to reduce the chances of abuse of a director's position (Douglas 1934).

Typically, directors are recognised as owing duties of loyalty and care, as well as various other subsidiary duties (such as duties of disclosure, maintaining appropriate standards of care, etc.).[173] The fiduciary duty owed by directors were traditionally directed *solely* towards the company concerned. However there has been a shift in the law to broaden the scope of a director's duties towards other stakeholders in society.[174]

The range of interests recognised under the Companies Act, 2013, brings with it a question as to an order of preference in case of conflicts. In this regard, one may refer to the position in the United Kingdom (as Section 166 of the Companies Act is based on Section 172 of the UK Companies Act, 2006).[175] Under the English approach, the primary duty of directors is towards the long-term interests of the company, but they also owe a secondary duty to certain outside stakeholders (Cabrelli and Esser 2018) and (Henderson 2009).

We now move on to illustrate the specific duties of directors recognised under Indian company law.

- **Limitation of authority:** Per Section 166(1) of the Companies Act, directors of a company are required to act within the limits of the authority conferred on them by the articles of the company. In general, the powers of a director are co-extensive with that of the company.[176]

172 A company cannot act for itself and neither can its shareholders be expected to practically or effectively supervise every action taken by a director on a daily basis (Radhabari Tea Co Pvt. Ltd. vs. Mridul Kumar Bhattacharjee and Ors. 2009).

173 Refer to (Mohmad Rafiq Jafferbhai Bagwan v. Sathyaprakash Subramanian and Others 2012) for a summary of the director's fiduciary duties.

174 For instance, the Companies Act, 2013 in Section 166(2), requires directors to act in good faith and to promote the objects of the company, *"for the benefit of its members as a whole, and in the best interests of the company, its employees, the shareholders, the community and for the protection of the environment."*

175 The UK, rather than adopting a focus on the shareholders of the company (often referred to as the "shareholder primacy approach") or requiring a range of different stakeholders to be placed on par with each other, adopts an "enlightened shareholder value" approach, which recognises broader social interests - while still attempting to place the company itself in the primary position of beneficiary (Williams 2012).

176 They cannot however exercise powers exercisable by shareholders at general meetings. Refer Section 179 of the Companies Act, 2013.

Directors can be held liable for acting beyond their delegated powers, even if such acts are within the general authority of the company itself (In Re: Oxford Benefit Building and Investment Society 1886). In situations where the director acts outside his or her authority, they can be liable to compensate the company for losses (Ramaiya 2014).

- **Duty of loyalty / No conflict:** The duty to act in good faith and for the benefit of the company is one of the most important of a director's duties. This duty is recognised in numerous provisions of the Companies Act, 2013, notably in Sections 166(2) and (4) thereof.[177] Section 166(5), Companies Act, 2013, also specifies that a director should not achieve or attempt to achieve any undue gain or advantage either to himself or to certain related parties and if found doing so, is liable to account for the same.[178]

  The statute is clear in not just requiring directors to avoid a direct conflict of interest - but also stops them from entering situations where there is a mere possibility of such a conflict.Director's may however engage in such transactions, subsequent to adequate and specific information being provided to the company, and consent being obtained.[179]

  To illustrate, one may examine the case of a director's powers to issue further capital. Courts have uniformly held that this power, by virtue of being exercised in a fiduciary relationship, can only be used in the interests of the company itself.[180] The power to issues shares cannot be used by the director to directly seek to enrich himself at the cost of the company. In situations where the director profits as a result of the exercise of powers, this would only be valid if this benefit is incidental

177 These provisions convert longstanding common law duties into statutory ones by requiring directors to act in "good faith" to promote the objects of the company and by prohibiting the director from acting in situations where he or she may have a conflict of interest with the company.

178 This position is similar to that under Section 88 of the Trusts Act.

179 As an aside, section 197 of Companies Act also limits the possibilities of a director taking advantage of a company by capping the maximum managerial remuneration. Any sums recieved by the director above the prescribed limits are to be held in trust for the company.

180 Refer (Nanalal Zaver and Ors. v. Bombay Life Assurance Co. Ltd. and Ors. 1950), (Needle Industries (India) Ltd. and Ors. v. Needle Industries Newey (India) Holding Ltd. and Ors. 1981) and (Ram Parshotam Mittal and Ors. v. Hotel Queen Road Pvt. Ltd. and Ors. 2019).

and not the main motive of the further issue.[181] The exercise of such powers must be bona fide[182] and must be done with a proper motive i.e. for reasons that place the beneficiary's interests first.[183]

- **Standard of care:** A director is required to undertake his or her work with reasonable care and by exercising due diligence as appropriate in the facts of the matter.[184]

  Section 166(3) of the Companies Act, 2013, makes it incumbent on the director to "exercise his duties with due and reasonable care, skill and diligence". Courts have often hightened the requirement to impose requirements of acting with "utmost skill, care and diligence" (N. Narayanan v. Adjudicating Officer, SEBI 2013) and (Ajay Surendra Patel v. Deputy Commissioner of Income Tax 2017).

- **Reducing information asymmetry:** As one of the primary ways in which the possible abuse of powers by a fiduciary can be checked, the Companies Act casts numerous duties of disclosure on directors.These include Sections 170, 184, 189, 129, and 102 which require a range of disclosures to be made by directors to the company pertaining to their identities, interests held by them and possible conflicts, the status of the company, etc. Failure to make a disclosure can lead to punitive action and the requirement to hold any profits in constructive trust for the company.

  The duties of disclosure appear particularly important when one considers for instance, that certain acts comitted by a director that could be viewed as a breach of fiduciary duty can be saved through appropriate disclosures of material facts followed by consent of the company.

181 Refer (Ram Parshotam Mittal and Ors. v. Hotel Queen Road Pvt. Ltd. and Ors. 2019) and (Needle Industries (India) Ltd. and Ors. v. Needle Industries Newey (India) Holding Ltd. and Ors. 1981).

182 There must be a genuine need for the company to undertake the exercise of issuing shares (though this may not need to be limited to the raising of capital).

183 That is, it should not be done to maintain the director's own standing in the company or to limit the powers of specific shareholders, etc. (Dale and Carrington Invt. (P) Ltd. and Ors. v. P. K. Prathapan and Ors. 2005).

184 For instance, directors are required to inform themselves "prior to making a business decision, of all material information reasonably available to them." (Smith v. Van Gorkem 1985). In exercising their discretion, they must ensure "just and proper consideration" to the facts and circumstances of the case. They must act bona fide and not arbitrarily and not for any collateral motive, but solely in the interest of the company (Smt. Bina Barua and Ors. v. Dalowjan Tea Co. (P.) Ltd. and Ors. 1981).

- **Confidentiality:** Directors are likely to come across sensitive commercial and trade related information in the course of their activities, and such information is generally exchanged in circumstances where there is an expectation of privacy.Therefore a fiduciary duty is imposed on them to keep such information secret, and particularly not disclose or use it for their own benefit without the company's consent. Information that is public or general knowledge is not subject to confidentality requirements, even if learnt during the course of directorship (EV Motors India Pvt. Ltd. v. Anurag Aggarwal and Ors. 2017).[185]

  A director who uses a company's confidential information for his own personal purposes is said to have misappropriated company assets and is therefore accountable to it for the same (Boardman v Phipps 1966), (Fairfest Media Ltd. vs. ITE Group Plc. 2015)and (Exchange Telegraph Co. Ltd. v Gregory and Co 1896).

  The duty to maintain confidentiality does not end with directorship - but only when the director is specifically released from the obligation or the information becomes a matter of public knowledge (Morrison v Moat 1851) and (Independent Broadcasting Company Ltd. v. Rob McKay (Media) Ltd. 1991).[186]

- **Remedies:** The law recognises a range of remedies against directors who act in breach of their fiduciary duties.[187] This may range from the ability of a corporation to avoid certain agreements or actions, to punitive action (such as imprisonment and fines) or termination of directorship / removal from office. Often, particularly in cases where the director has profited at the expense of the company, courts may deem a constructive trust to be created and require the director to account to the company for any illegal gains.

  Per the Companies Act, 2013, remedies will usually be enforced by a special tribunal.[188]

185 As far as statutory recognition of the duty of confidentiality is concerned, one may for example, look towards Sections 194 and 195 of the Companies Act which prohibit directors from engaging in forward dealing or insider trading.

186 This position is subject to the statory requirements in Indian law that prohibit contracts in restraint of trade.

187 An action may be brought against a director on behalf of the company as well as shareholders in certain cases.

188 Section 430 of the Companies Act ousts the normal jurisdiction of civil courts over matters which the company law tribunal and appeals tribunal is empowered to adjudicate. The government may also establish special courts to try certain specific offences under the law. Section 463 of the Companies Act recognises that despite negligence, default, breach of duty or misfeasance or breach of trust commited by the director, he or she may indeed have acted honestly and reasonably, in which case courts may relieve the director of liability.

6.3. Doctor-patient relationships

Doctor-patient relationships have often been referred to as fiduciary by Indian courts.[189] However, this appears largely a formulaic rendering. English common law does not specifically recognise doctors as fiduciaries (Sidway v. Bethlem Royal Hospital Governors 1985). It has been suggested that common law has other suitable remedies to protect patients, and that deeming the relationship as fiduciary would entrench paternalism in English law thereby limiting the agency of patients (Bartlett 1997) and (Kennedy 1996). The United States and Canada however do recognise a doctor as a fiduciary. Patients entrust their bodies to the doctor leading to the creation of a power asymmetry between the two. There is also information asymmetry due to the difference in knowledge and experience. A doctor can act unilaterally to the patient's detriment. They are therefore required to act with duties of good faith and loyalty.[190] India does however, impose fiduciary duties on doctors through statute. We briefly discuss these below.

- **Duty of loyalty / No conflict:** Doctors are typically required to place the patient's considerations over others, including their own.[191] This principle is recognised in the law, for instance the IMC Regulations provide that the personal financial interests of a physician should not conflict with the medical interests of patients.[192] Doctors having an incapacity "detrimental to the patient" or which can affect performance of duties are not permitted to practice.

  The duty to avoid a conflict of interest and to place a patient's interests first has come under increasing challenge due to the growing enterpreneurial interests in medicine. Though not per se barred from indulging in practices that seek

189 See for example (Secretary General, Supreme Court of India v. Subhash Chandra Agarwal 2010) and (Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors. 2012).

190 See (Frankel 2011), (Moore v. Regents of University of California 1990), (Miller v. Kennedy 1987), (Norberg v. Wynrib 1979) and (Mclnerney v. MacDonald 1992).

191 Refer for instance to the modern Hippocratic oath which states that "The health and well being of my patient will be my first consideration" and the original version which provides "…I will do no harm or injustice to them… Into whatever homes I go, I will enter them for the benefit of the sick, avoiding any voluntary act of impropriety or corruption, including the seduction of women or men, whether they are free men or slaves" (Parsa-Parsi 2017) and (North 2002).

192 For instance, regulation 1.1.2 recognises that financial gain should be a subordinate interest to the patient's well being. Doctors are also beholden to remember that patients depend on them.

to enrich themselves, doctors must provide sufficient information about any conflicting interests so as to enable the patient to make an informed decision about the matter.[193]

Doctors may typically act against their patient's interests by:

- Providing excessive, insufficient or inadequate services;
- Charging excessive fees;
- Prescribing treatment in which the doctor has a direct or indirect interest;
- Referring patients, for a fee;

(Healey and Dowling 1991)

All these practices are regulated under medical law. For instance, doctors are required to announce their fees before rendering the service.[194] They must as far as possible recommend drugs using their generic names leaving it to the patient to choose a manufacturer and brand.[195] Doctors are also prohibited from accepting gifts in cash or kind from pharmaceutical and allied industries. They should ensure interests of patients are not compromised by virtue of affiliations with any industry groups. The MCI Regulations provide that a physician is not to solicit consideration for referrals or for recommending any treatment for a patient.[196] Unecessary consultations are to be avoided. The patient's benefit must be of foremost importance in conducting a consultation.

- **Standard of care:** Doctors are required to act with a "reasonable degree of skill and knowledge" and a "reasonable degree of care" (Laxman Balkrishna Joshi v. Trimbak Bapu Godbole 1969). The standard implies that doctors must exercise an ordinary degree of professional skill - that is, they must act in accordance with

193 In (Moore v. Regents of University of California 1990), the court held that the doctor was required to inform the patient of his interest in extracting his cells, before the conduct of an operation.

194 The remuneration should be in the form and amount specifically announced to the patient at the time service was rendered. Refer to regulation 1.8, IMC Regulations.

195 This reduces the incentive for doctors and pharmaceutical companies to collude.

196 The law however does not restrain doctors from attending industry events, accepting free samples etc. (ACIT v. Eli Lilly and Company India Private Limited 2019) and (ACIT2019 Indlaw ITAT 2730 v. Life Star Pharma Private Limited 2018).

what is commonly expected of an ordinary professional.[197] The Supreme Court has held that a difference of medical opinion would not be sufficient to hold the doctor as not fulfiling the duty of care, so long as the patient was attended to with "due care, skill and diligence" (Achutrao Haribhau Khodwa v. State of Maharashtra 1996).[198] The duties of a doctor towards a patient are personal, and cannot be delegated (Spring Meadows Hospital v. Harjot Ahluwalia 1998).

- **Reducing information asymmetry:** Medical law places significant emphasis on the notice and consent framework to protect user rights and to this end requires disclosures to be made "in the best interests" of the patient.[199] Prior to securing consent, it is vital that doctors provide sufficient information to patients so as to enable an informed choice. Doctors must also confirm that patients are in a position to understand the information provided to them and properly evaluate risks.[200] The law also requires hospitals to use specified templates to display and provide various types of information concerning patient rights and specific procedures.[201]

  Consent must be obtained before commencing treatment. The patient should have capacity and competence to consent, it should be voluntary, and consent should be on the basis of adequate information (Dr. Prabha Manchanda 2008). Consent has to be specific in nature and cannot be used to encompass even treatments that may be beneficial to the patient (Dr. Prabha Manchanda 2008).

  The Supreme Court considered two possible standards of consent in (Dr. Prabha Manchanda 2008): 'informed consent' and 'valid consent'. The former implies informing the patient of "all risks potentially affecting the decision".[202] The

197 The Hippocratic Oath in its latest form requires doctors to act with "conscience and dignity and in accordance with good medical practice." (Parsa-Parsi 2017).

198 Differences of opinion need not be always disclosed. However, if they are irreconcilable in nature, the competing options should be frankly and impartially explained to the patient.

199 Refer for instance to Regulation 2.3 of the MCI Regulations. This is based on the moral conviction that everyone has a right of self determination with regard to his body, and to protect his or her body integrity against invasion by others. In certain cases, treatment without a lack of consent can render the physical invasion criminal (Schloendorff v. Society of New York Hospital 1914).

200 The patient must be able to (a) comprehend and retain the relevant information, (b) believe it, and, (c) weigh it in the balance so as to arrive at a choice (Re C (Adult: Refusal of Medical Treatment) 1994).

201 Refer for instance to regulation 9 of the Clinical Establishments (Central Government) Rules, 2012.

202 See (Canterbury v. Spencer 1972), (Reibl v. Hughes 1980) and (Rogers v. Whittaker 1992).

latter standard, which was finally adopted by the court, implies that sufficient information should be given that would enable a reasonable assessment by the patient of the risks of treatment.[203] The doctor should should disclose as much information as per practice commonly accepted in the profession. He or she has discretion to disclose relevant facts given the circumstances at hand and keeping in mind the best interests of the patient. Full disclosure of all *facts* is not required.[204] Information on the nature and procedure of treatment (purpose, benefits, effects), alternatives, substantial risks and possible adverse consequences of refusing treatment must be provided to the patient (Dr. Prabha Manchanda 2008).

Doctors are also obliged to provide the patient with his or her own medical records, within a period of 72 hours from a request (Sameer Kumar v. State of Uttar Pradesh 2014).

Remedies for lack of disclosures or proper consent can lie in specific statutes, consumer protection law and tort.[205]

As an aside, doctors are not just required to provide information about their practice, but also have a fiduciary duty to "expose unethical or incompetent colleagues" (Frankel 2011). This duty is captured in the IMC Regulations.

- **Duty of confidentiality:** Confidentiality of health and treatment related information is a core principle in the doctor-patient relationship.[206] It allows patients to confide in their doctor, enabling proper diagnosis and treatment.

203 Refer to (Bolam v. Friern Hospital Management Committee 1957), (Sidway v. Bethlem Royal Hospital Governors 1985) and (Pearce v. United Bristol Healthcare NHS Trust 1998).

204 The "informed consent" standard was held to be impractical as: (a) it does not pay due heed to the doctor's judgment regarding the risks the patient should be told about, that the doctor's clinical judgment is important as to what risks the patient should be apprised of since it may unduly influence the patient's calculations, second, (b) it would negate the benefit of djudging the disclosure per medical practice; (c) the "objectivity" of of the test was imprecise as it required judges to decide what a "reasonable" patients position would be; and, fourth, as it may increase costs of treatment due to the higher standards required.

205 Refer to (Nizam's Institute of Medical Sciences v. Prasanth S. Dhananka 2009) and (Sameer Kumar v. State of Uttar Pradesh 2014).

206 For example, the original Hippocratic oath provides "And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets." The most modern version from 2017 states "I will respect the secrets that are confided in me, even after the patient has died" (North 2002) and (Parsa-Parsi 2017).

There multiple sources of law including tort and statute, that recognise doctor's duties of confidentiality. For example, the Medical Health Act, 2017, requires health professionals to keep information obtained during care or treatment confidential. The law however recognises various exceptions to this - including if disclosure is required to enable another medical professional to provide services, prevents harm to the patient, is required in public interest or to a representative of the patient.[207] Similarly the IMC Regulations requires doctors not to disclose secrets of a patient except in accordance with public interest exceptions.[208] There is also a prohibition on publishing photographs or case reports of the patients, in a manner that their identity would be made out, without their permission. Certain laws such as the Electronic Health Record Standards, Version 2016, require data protection standards to be maintained with respect to electronic health records.

- **Remedies:** Remedies available to patients for breach of duties by a doctor can be in the form of actions for damages under tort, contract and statutes such as the Consumer Protection Act and even the Penal Code). The Medical Council can also take disciplinary action against doctors for violating their professional conduct rules.

207 The proposed Draft Information Security in Healthcare Act (DISHA), also codifies duties of confidentiality pertaining to digital health data. Notably, Section 28 recognises that the owner of the data shall have rights to privacy, confidentiality and security of the data. The Code of Medical Ethics Regulations, 2002, requires confidentiality of information entrusted to doctors, unless required by law.

208 Which include by order of a court of law, in circumstances where there is a serious and identified risk to a specific person and/or community, or in case of notifiable diseases.

7. Annexure - II: Summary comparison of the PDP Bill with the GDPR

Scope of Protections		
	GDPR	*PDP Bill*
Nature of data protected	Information relating to identified or identifiable natural persons. Does not cover nonpersonal data, anonymised data. Covers manual processing where the processing forms part of a filing system.	Information relating to directly or indirectly identifiable natural persons. Does not cover non-personal data, anonymised data. Covers manual processing except by small industries.
Territorial Application	Applies to processing in the context of activities of a controller in the EU, irrespective of where the processing occurs.	Applies to processing carried out in connection to a business carried out in India, or where Indian data principals are profiled.
Processing entity	Controller = entity or person who alone or with others, determines purposes or means of processing personal data.	Data fiduciary = entity or person who alone or with others, determines the purpose and means of processing personal data.
Subject of protection	Data subject = the natural person to whom any information relates to or identifies or through which he/she is identifiable.	Data principal = the natural person who personal data relates to.

General Principles of Processing	
GDPR	*PDP Bill*
Processing to be *lawful, fair and transparent*	Processing to be *fair and reasonable.*
Processing to be for explicit, specified and legitimate purposes. Further processing to be compatible with initial purposes *(purpose limitation).*	Processing only for purposes that are clear, specific, lawful. Further processing permitted where incidental to original purpose and such that this can be reasonably expected by the data principal *(purpose limitation).*
Requirement of valid ground for processing to be lawful.	Requirement of valid ground for processing to be lawful.

General Principles of Processing	
GDPR	*PDP Bill*
Only that data to be processed as is adequate, relevant and limited to what is necessary in relation to the purposes of processing *(data minimisation)*.	Only that data to be collected which is necessary for the purpose of processing *(Collection limitation)*.
Personal data to be accurate and up-to-date. Reasonable steps to be taken to delete inaccurate data *(accuracy)*.	Data fiduciary to take reasonable steps to ensure that personal data is complete, accurate, updated *(Data quality)*.
Personal data to be retained in identifiable form for as long as necessary to fulfil purpose of processing. *(Data storage limitation)*.	Data to be stored (in identifiable form) only for as long as required to fulfil a purpose for which it is processed. *(Data storage limitation)*.
Processing to take place in a manner that ensures security of the personal data including protection against unauthorised use, loss, destruction, unlawful processing etc. *(integrity and confidentiality)*.	Appropriate *security safeguards* to be implemented in view of the nature, scope and purpose of processing and risks of harm.
Data controller to be responsible for compliance *(accountability)*.	Data fiduciary responsible for compliance with the law and to demonstrate the same *(accountability)*.

Valid Consent	
GDPR	*PDP Bill*
Free	Free
Demonstrable (onus on data controller)	Demonstrable (onus on data fiduciary)
Data subject must be informed of the fact that consent is being taken, a long list of information is also to be provided at the time of taking consent. Notably, this list includes information on the the existence of automated decision making, which is not a specific requirement in the Indian law. In this regard, the logic involved, significance and possible consequences must also be shared.	Long list of information to be provided by data fiduciary at time of taking consent. Notably this includes data trust scores of data fidiciaries, which is not present in the European law.
Intelligible and easily accessible	Clear
Clearly distinguishable	Specific
Capable of being withdrawn as easily as it was given	Capable of being withdrawn as easily as it was given

Valid Consent	
GDPR	*PDP Bill*
Service provision should not normally be contingent on having to provide unecessary personal data	Service provision cannot be contingent on having to provide unecessary personal data
Explicit consent required to process sensitive personal data. Explicit consent also required for any automated processing that involves decision making about an individual (including by profiling)	Explicit consent required to process sensitive personal data. No such requirement for automated decision making.
Explicit consent not specifically defined	Explicit consent requires higher standards of specificity, information and clarity than otherwise provided in the law.
Notice to be provided at the time data is collected	Notice to be provided at the time data is collected.
Exceptions to notice requirements apply where this would involve disproportionate effort, processing is for public interest archiving, scientific, historical research or statistical purposes, or where there is a confidentiality requirement in the law.	Exceptions to notice requirements when data is to be processed for prompt action.

Grounds for Processing	
GDPR	*PDP Bill*
Consent / explicit consent for sensitive data, must be capable of being withdrawn	Consent / explicit consent for sensitive data, must be capable of being withdrawn
For performance of a contract	-
For compliance with legal obligation of the data controller	For compliance with legal obligation imposed by a law, or orders of a court/tribunal
Necessary to protect vital interest of data subject or another person	Necessary for prompt action in cases of medical emergency (of any individual), to deal with public health emergencies, or other public safety and public order issues
Necessary to carry out a task in public interest or in exercise of official authority	Necessary for functions of the state

Grounds for Processing	
GDPR	*PDP Bill*
Necessary for legitimate interests of the data controller, except where overridden by the interests or rights of the data subject	Processing for reasonable purposes as may be specified by the data protection authority
No separate ground for employment related processing, members states may lay down additional safeguards for processing in these contexts	Processing for employment related purposes recognised as a specific ground

Processing of Sensitive Personal Data	
GDPR	*PDP Bill*
Sensitive personal data include personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. Additionally, if genetic data, biometric data is used for the purposes of identifying natural person, health, sex life or sexual orientation	Includes passwords, financial data, health data, official identifiers, sex life, sexual orientation and another 6 categories of data. The data protection authority can expand the list of categories.
Imposes a general prohibition on processing of sensitive data, unless one of ten exceptions is met including explicit consent	Does not impose a general prohibition on processing. However, allows processing subject to explicit consent, if strictly necessary for exercise of state functions (authorised by law for service provision to the data principal), to comply with the explicit mandate of any law or court orders, and where necessary for prompt action.

Rights of Individuals	
GDPR	*PDP Bill*
Right to confirmation about processing	*Right to confirmation* about processing
Right of access provided. Copy of personal data to be made available at a reasonable cost.	*Right of access provided.* Brief summary of data being processed, and method of processing to be provided. Reasonable fee can be charged.
Right to correction provided. Data controller to inform recipients of corrections.	*Right to correction provided.* Data fiduciary to notify recipients of corrections.
Right to data portability provided with certain limitations such as where processing is in public interest, or in consonance with official authority vested in the controller.	*Right to data portability* provided with some limitations for processing for functions of the state, for processing in compliance with a law or other legal obligations

Rights of Individuals	
GDPR	*PDP Bill*
Right to object to processing provided in case of processing in public interest or for legitimate interests of data controller. Specifically made available for processing related to direct marketing. Right not available where processing or archiving for public interest, scientific or historical research purposes.	No specific right to object. Data principal can only withdraw consent to processing.
Profiling is prohibited if it produces legal effects or significantly harms the data subject. Exceptions are also provided to this (explicit consent, performance of contract, permitted by a law).	DPA can prohibit certain practices that have a likelihood of causing harm (subsequent to submission and scrutiny of a data protection impact assessment).
Right of erasure provided on 6 grounds. Where the personal data is already made public, data controller to take measures to limit continued availability / processing of the data (subject to appropriate balancing of interests)	Data principal has the *right to restrict or prevent continuing disclosure* of personal data on 3 grounds and subject to appropriate balancing of interests. No specific right of erasure and no requirement for the data fiduciary to inform other data controllers to restrict availability of the personal data.
The GDPR recognises a specific *right against automated individual decision making incuding profiling.* This is subject to various exceptions	No specific right against automated individual decision making. The data protection authority may require amendment of, bar or specify safeguards in respect of any practices

Exemptions	
GDPR	*PDP Bill*
Proportionate exemptions permitted under laws where processing concerns national security and defence *(security of state).*	Proportionate exemptions permitted under a law that lays down appropriate procedural safeguards *(security of state).*
Public security, prevention / detection / investigation / prosecution of criminal offences, preventing threats to public security, prosecution of breaches of ethics for regulated professions *(law enforcement).* / prosecution of any offence or contravention of law. Data to be retained only if it is a proportionate measure for preventing an offence *(law enforcement).*	For prevention / detection / investigation

Exemptions	
GDPR	*PDP Bill*
Protection of judicial independence and judicial proceedings, enforcement of civil law claims *(legal proceedings).*	Enforcing any legal right or claim, seeking any relief, defending any charge, opposing any claim, obtaining legal advice from an advocate *(legal proceedings).*
Research, archiving or statistical purposes	Research, archiving or statistical purposes
Personal or household purpose	Personal or domestic purpose
Member states to balance journalistic interests with privacy interests	Exemption for journalism subject to certain conditions
Exemption to provide the public access to public / official documents	Exemption in the case of documents under the Right to Information Act, 2005
States to lay down specific laws for processing of national identification numbers	State can implement laws for processing of national identification numbers, but no specific provision in the draft law
Exemptions in the case of professional rules of confidentiality and in case of confidentiality rules of religious organisations	-
Entities with less than 250 employees not required to maintain records unless there is a risk of privacy harms. No exemption for manual processing	Law contains exemptions for manual processing by small entities (the phrase small entity is defined not in accordance to employee numbers but by turnover, number of individual's whos data is processed, etc.)

Transparency, Security and Accountability Measures	
GDPR	*PDP Bill*
Data controllers to implement *privacy by design.*	Data fiduciaries to implement *privacy by design.*
Data controllers / processors to *maintain records* of purpose of processing, categories of recipients of data, categories of data with controller etc. This requirement is not mandated for data controllers with less than 250 employees unless the risks posed by such processing are high	Data fiduciaries / processors to *maintain records* of purpose of processing, categories of recipients of data, categories of data with controller etc. Additional record keeping obligations are specified for significant data fiduciaries.
Security safeguards proportionate to nature of risk to be implemented	Security safeguards proportionate to nature of risk to be implemented

Transparency, Security and Accountability Measures	
GDPR	*PDP Bill*
Data breach notification to data subjects where the breach is likely to result in a high risk to rights of data subject. No requirement of notification where this would involve disproportionate effort, or where risks are negated due to remedial measures implemented by data controller, or where data is encrypted. Notification to supervisory authorities is required.	Data fiduciary to *inform data protection authority* in case of breach is likely to cause harm to data principals. Data protection authority to determine if data principal should be informed.
Supervisory authority to specify which activities require a data protection impact assessment *(DPIA).* DPIA to be required based on risks of harm. The authority may require the processing activity to be modified under A 58.	*DPIA* required in all cases of processing by a "significant data fiduciary" (or as otherwise required by the data protection authority), where there is a risk of significant harm or as notified by the authority. The data protection authority will review all DPIAs. It can order modification or a bar on processing activities that are likely to cause harm to data principals.
Requirement of certification including in the form of data protection seals and marks. Certification requirements to be proportionate and voluntary.	Requirement of *data audits* for significant data fiduciaries (or those otherwise required to do so by the data protection authority) by an independent auditor including giving data fiduciaries a *data trust score* which they must inform to data principals (in notices, etc).
Data protection officers to be appointed to monitor compliance, provide advice, take complaints from individuals, and liaise with supervisory authority	*Data protection officers* to be appointed by significant data fiduciaries (or as otherwise specified by the data protection authority) to monitor compliance, provide advice, take complaints from individuals and liaise with supervisory authority
Codes of conduct to be prepared by the market/industry, which will then be approved by the supervisory authority	*Codes of practice* to be prepared by the data protection authority or p[repared by industry and approved by the authority
Provision for prior consultation with supervisory authority on legality of processing practices.	-
Data protection officers can be approached to lodge complaints. There is however no detailed grievance redress process provided.	Data protection officers to take complaints from data principals. Requirement for data fiduciaries to have a *grievance redressal mechanism* with specified period to deal with complaints, etc.

Miscellaneous Provisions	
GDPR	*PDP Bill*
No specific definition of harms in the operative provisions of the GDPR. Penalties apply for breach of the law. Compensation is payable in case of material or nonmaterial damage to the data subjects. The recitals to the GDPR indicate the nature of harmful processing including practices that give rise to discrimination, identity theft, fraud, financial loss, unauthorised reversal of pseudonymisation, etc.	Lists and grades harms into "harms" and "significant harms" (aggravated form of harms having regard to the risks involved in the processing). The concept of harm is used to determine applicable obligations (eg: privacy by design should aim to reduce harms, security standards should be based on severity of harm that may occur, requirement for data breach notification is based on likelihood of harm, etc.) and certain actions by the data protection authority. Complaints can be raised by the data principal where there is a likelihood of harm. The significant harm standard is used as a determinant for certain additional obligations for data fiduciaries (eg: data protection impact assessment requirement, additional transparency obligations, etc.), and actions by the data protection authority (eg: notification of additional categories of sensitive personal data, prohibiting practices where there is a risk of significant harm to children, notifying data fiduciaries as significant data fiduciaries, etc).
Additional protections in the law for *children* under 16 years. Consent for children below 16 has to be given by a guardian. Notice must be provided in a child friendly manner, and legitimate interests of a controller cannot override a child's rights	Additional protections in the law for children under 18 years, with guardian consent required in such cases. High standard of protection provided as data fiduciaries are required to process information in the "best interests" of children. Law permits notification of *"guardian data fiduciaries"* who are barred from processing practices that could cause significant harm such as profiling, tracking, directing targetted advertising to children or carrying out behavioural monitoring.
Cross border transfers permitted without authorisation where adequacy decision made by EU Commission, and subject to safeguards. In case no adequacy decision is made, transfers permitted based on consent, subject to appropriate safeguards such as binding corporate rules, necessity in public interest, required for performance of a contract, etc.	Requirement to completely localise or mirror certain notified types of personal data. Data that does not have to be localised can be transferred subject to consent, authorisation of the data protection authority, adherence to safeguards such as binding corporate rules, etc.

Remedies and Penalties	
GDPR	*PDP Bill*
Liability arises for breach of law. Compensation payable for causing material or non-material damage.	Liability arises for breach of law or on causing harm. Compensation payable based on harm caused.
No criminal liability	Criminalises certain violations of the law such as obtaining, transferring or selling of personal and sensitive personal data in contravention to the law and re-identification of data without the consent of data fiduciary or processor.
Graded penalties based on nature of contravention and other factors such as previous infringements, cooperation with supervisory authority etc. Maximum penalty payable for violation of the law is EUR 2 million (INR 155.5 million) or 4 percent of the total worldwide annual turnover	Graded penalties based on nature of contravention. Maximum penalty payable for violation of the law is INR 150 million or 4 percent of total worldwide turnover.
Grounds for compensation include material or non-material harm suffered by the data subject Primary adjudicatory forum (for compensation) is the civil court	Compensation is payable in view of harm caused to data principal Jurisdiction of civil courts is ousted. Compensation claims lie before the Adjudicatory Authority established under the draft law.

Powers of the Regulatory Authority	
GDPR	*PDP Bill*
-	Can specify "reasonable purposes" of processing, as a non-consent based ground for processing
Can restrict data processing practices due to likelihood of harm	Can restrict data processing practies due to likelihood of harm
-	Can notify data fiduciaries as "significant data fiduciaries" which requires compliance with additional obligations

Powers of the Regulatory Authority	
GDPR	*PDP Bill*
The EU Commission can make adequacy decisions to indicate if a country's data protection laws are sufficiently strong so as to permit eased data transfers. The supervisory authority can lay down / approve standard clauses and binding corporate rules to enable cross border transfers. Controllers are also required to inform supervisory authorities of certain types of transfers. The authority can also suspend or discontinue cross border data transfers	Central government can notify categories of data to be stored only in India. It is also to make adequacy decisions in consultation with the data protection authority. The authority is required to approve intragroup schemes and can approve transfers on grounds of necessity. The authority can also suspend or discontinue cross border data transfers
Can issue warnings, reprimands and directions for compliance	Can issue warnings, reprimands and directions for compliance
To be informed of data breaches and can order communication of the same to the data subject	To be informed of data breaches. Decides whether to communicate this to the data principal.
Can amend processing practices or bar a practice	Can amend processing practices or bar a practice
Can order rectification or erasure of personal data	Can require compliance with the law (which enables rights of rectification and requires deletion of data after it has served its purpose).
Investigate complaints, conduct inquiries, etc. Has powers of search and seizure and can call for information	Investigate complaints, conduct inquiries, etc. Can carry out search and seizures and call for information
Encourage drawing up of codes of conduct and establishment of certification mechanisms, accredit bodies to monitor codes of conduct	Can mandate use of specific forms for notices, empanel data auditors, prescribe codes of practice
Can handle complaints	Adjudicatory Authority handles complaints

References

Achutrao Haribhau Khodwa v. State of Maharashtra (1996). [1996] 2 SCR 881.

ACIT v. Eli Lilly and Company India Private Limited (2019). 2019 Indlaw ITAT 2730.

ACIT2019 Indlaw ITAT 2730 v. Life Star Pharma Private Limited (2018). 2018 Indlaw ITAT 9784.

Ajay Surendra Patel v. Deputy Commissioner of Income Tax (2017). [2017] 202 CompCas 179 (Guj).

Ames, James Barr (1908). "The origins of uses and trusts". In: *Harvard Law Review* 21.4. URL: http://tiny.cc/ub75az.

Anonymous (2019). *GDPR in numbers.* URL: https://ec.europa.eu/commission/sites/beta-political/files/190125_gdpr_infographics_v4.pdf.

Association of Unified Telecom Service Providers of India v. Union of India (2014). 207 (2014) DLT 142.

Bailey, Rishab and Smriti Parsheera (2018). *Data localisation in India: Questioning the means and ends.* URL: https://macrofinance.nipfp.org.in/releasesZBP2018_Data-localisation-in-India.html.

Bailey, Rishab, Smriti Parsheera, Faiza Rahman, and Vrinda Bhandari (2018). *Comments on the (Draft) Personal Data Protection Bill, 2018.* Comments submitted to the Ministry of Electronics and IT, Government of India. URL: http://tiny.cc/3nlj7y.

Bailey, Rishab, Smriti Parsheera, Faiza Rahman, and Renuka Sane (2018). *Disclosures in privacy policies: Does notice and consent work?* NIPFP Working Paper No. 246. URL: https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf.

Balkin, Jack (2014). *Information Fiduciaries in the Digital Age.* URL: https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html.

Balkin, Jack M (2018). *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation.* UC Davis Law Review. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3038939.

Balkin, Jack M (2016). *Information fiduciaries and the first amendment.* URL: https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf.

Balkin, Jack M (2018). *Fixing Social Media's Grand Bargain.* URL: https://www.hoover.org/sites/default/files/research/docs/balkin_webreadypdf.pdf.

Balkin, Jack M and Jonathan Zittrain (2016). URL: https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/.

Bambauer, Jane (2016). *The relationships betweenfree speech and conduct.* URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2788248.

Bartlett, Peter (1997). "Doctors as Fiduciaries: Equitable Regulation of the Doctor Patient Relationship". In: *Medical Law Review* 5.

Berkeley Community Villages Ltd and Anr. v. Pullen and Ors. (2007). [2007] EWHC 1330 (Ch).

Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors. (2012). (2012) 13SCC61.

Boardman v. Phipps (1966). (1966) 3 All ER 721.

Bodil Lindqvist v. Aklagarkammaren i Jonkoping (2003). Case C-101/01, CJEU.

Bolam v. Friern Hospital Management Committee (1957). [1957] 1 WLR 582.

Cabrelli, David and Irene-Marie Esser (2018). "A rule based analysis and comparison of case studies". In: *Comparative company law: A case based approach.* Ed. by M Siems and David Cabrelli. Oxford: Hart Publishing.

Canbank Financial Services Ltd. v. Custodian and Ors. (2004). (2004) 8 SCC 355.

Canterbury v. Spencer (1972). 464 F2d 772 (DC Cir 1972).

Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors. (2011). (2011) 8 SCC 497.

Clarry, Daniel (2014). "Fiduciary ownership and trusts in a comparative perspective". In: *International and Comparative Law Quarterly* 63.4. URL: https://www.researchgate.net/publication/280233557_Fiduciary_ownership,and_trusts_in_a_comparative_perspective.

Crowther, BT (2012). "(Un)Reasonable expectation of digital privacy". In: *BYU Law Review* 2012.1. URL: http://tiny.cc/7ptabz.

Dale and Carrington Invt. (P) Ltd. and Ors. v. P.K. Prathapan and Ors. (2005). AIR 2005 SC 1624.

Davis, Seth (2014). "The False Promise of Fiduciary Government". In: *Notre Dame Law Review* 89.3. URL: https://www.ssrn.com/abstract=2434089.

Dinshaw Maneckji Petit v. Jamsetji Jeejeebhoy (1909). (1909) 2 Ind Cas 701.

Dobkin, Ariel (2018). *Information Fiduciaries in Practice: Data Privacy and User Expectations.* URL: http://btlj.org/data/articles2018/vol33/33_1/Dobkin_Web.pdf.

Douglas, William C (1934). "Directors who do not direct". In: *Harvard Law Review* 47.

Dr. Prabha Manchanda, Samira Kohli v. (2008). (2008) 2 SCC 1.

Dubroff, Harold (2006). "The Implied Covenant of Good Faith In Contract Interpretation and Gap Filling: Reviling a Revered Relic". In: *St. John's Law Review* 30.2. URL: http://tiny.cc/xngabz.

Editorial Board (2018). *How to Make Facebook and Google Behave.* Bloomberg Opinion. URL: https://www.bloomberg.com/opinion/articles/2018-04-24/make-facebook-and-google-information-fiduciaries.

EV Motors India Pvt. Ltd. v. Anurag Aggarwal and Ors. (2017). CS (OS) NO. 671/2017, Del High Court.

Exchange Telegraph Co. Ltd. v. Gregory and Co (1896). (1896) 1 QB 147.

Ezra, Jeri Beth K (1989). "The trust doctrine: A source of protection for native american sacred sites". In: *Catholic University Law Review* 38.3. URL: http://tiny.cc/qnw8az.

Fairfest Media Ltd. vs. ITE Group Plc. (2015). 2015 (2) CHN (Cal) 704.

Fatima Fauzia and Ors. v. Syed Ul-Mulk and Ors. (1979). AIR 1979 AP 229.

Flannigan, Robert (2004). *The Boundaries of Fiduciary Accountability*. URL: http://tiny.cc/gbh4az.

Frankel, Tamara (1983). *Fiduciary Law.* URL: https://scholarship.law.berkeley.edu/californialaw-review/vol71/iss3/1/.

Frankel, Tamara (2011). *Fiduciary Law*. Oxford University Press.

Gellman, Barton and Sam Adler-Bell (2017). *The Disparate Impact of Surveillance.* URL: http://tiny.cc/o5tabz.

Government of India, Ministry of Electronics and IT (2017). *Office Memorandum: Constitution of a Committee of Experts to deliberate on a data protection framework for India.* No.3(6)/2017-CLES. URL: http://tiny.cc/bx776y.

Hay's Settlement Trusts, Re (1981). [1981] 3 All ER 786.

Healey, Joseph M. Jr. and Kara L. Dowling (1991). "Controlling Conflicts of Interest in the Doctor-Patient Relationship: Lessons from Moore v. Regents of the University of California". In: *Mercer Law Review* 42.3.

Henderson, Gail (2009). *The possible impacts of "enlightened shareholder value" on corporation's environmental performance.* URL: http://tiny.cc/7g59az.

Hurley, Mary C (2002). *The Crown's Fiduciary Relationship with Aboriginal Peoples.* URL: http://publications.gc.ca/Collection-R/LoPBdP/BP/prb0009-e.htm.

In Re: Oxford Benefit Building and Investment Society (1886). (1886) 35 ChD 502.

Independent Broadcasting Company Ltd. v. Rob McKay (Media) Ltd. (1991). 1991 (5) NZCLC 67.

Industrial Development Consultants v. Cooley (1972). [1972] 1 WLR 443.

Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd (1989). [1989] 1 QB 433.

Justice Srikrishna Committee (2017). *White Paper of the Committee of Experts on a Data Protection Framework for India.* White Paper of the Committee of Experts on a Data Protection Framework for India. URL: https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf.

Justice Srikrishna Committee (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians.* Report of the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. URL: http://meity.gov.in/writereaddata/filesZData_Protection_Committee_Report.pdf.

Kalman, Laurence (2019). "New European Data Privacy and Cyber Security Laws: One Year Later". In: *Communications of the Association for Computing Machinery* 62.4. URL: http://tiny.cc/uj59az.

Kapila Hingorani v. State of Bihar (2003). (2003) 6 SCC 1.

Kennedy, I (1996). "The Fiduciary Relationship and it's Application to Doctors and Patients, Wrongs and Remedies in the Twenty First Century". In: *Oxford University Press* 114.

Khan, Lina and David Pozen (2019). *A Skeptical View of Information Fiduciaries.* URL: http://tiny.cc/hhim7y.

Krishna Gopal Kakani v. Bank of Baroda (2001). CA No. 8448/2001, Supreme Court.

Langbein, John H (2005). "Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?" In: *Yale Law Journal* 114.1. URL: https://law.yale.edu/system/files/documents/pdf/Faculty/Langbein_Questioning_the_Trust.pdf.

Laudon, Kenneth C (1993). *Markets and Privacy*. Stern School of Business, Working Paper IS-93-21. URL: http://tiny.cc/cstn7y.

Law Commission of India (2006). *Unfair (procedural and substantive) terms in contract.* 199th Report of the Law Commission of India. URL: http://lawcommissionofindia.nic.in/reports/rep199.pdf.

Laxman Balkrishna Joshi v. Trimbak Bapu Godbole (1969). (1969) 1 SCR 206.

Leslie, Melanie (2005). "Trusting Trustees: Fiduciary Duties and the Limits of Default Rules". In: *Georgetown Law Journal* 94.1. URL: http://tiny.cc/czthbz.

Lightbourne, John (2017). "Algorithms and Fiduciaries: Existing and Proposed Regulatory Approaches to Artificially Intelligent Financial Planners". In: *Duke Law Journal* 3.67. URL: http://tiny.cc/qothbz.

M. Kanniyappan vs. The Presiding Officer, Labour Court and Ors. (2011). W.P. (MD) No. 4041/2006, Madras High Court.

Makkar, Angad Singh (2018). *Doctrine of Good Faith and Fair Dealing: Lacuna in Indian Contract Law.* URL: https://indiacorplaw.in/2018/12/doctrine-good-faith-fair-dealing-lacuna-indian-contract-law.html.

Mariyam Biwi v. Natharsa Rowther (1978). AIR 1978 Mad 244.

Matthan, Rahul (2017). *Beyond Consent: A New Paradigm for Data Protection.* URL: https://takshashila.org.in/discussion-document-beyond-consent-new-paradigm-data-protection/.

McInerney v. MacDonald (1992). (1992) 93 DLR (4th) 415.

Miller v. Kennedy (1987). 522 P. 2d. 852.

Miller, Paul B (2014). "The Fiduciary Relationship". In: *Philosophical Foundations of Fiduciary Law.* Ed. by Andrew S Gold and Paul B Miller. Oxford: Oxford University Press.

Mitchell, Charles (2010). Sweet and Maxwell, p. 354.

Mohmad Rafiq Jafferbhai Bagwan v. Sathyaprakash Subramanian and Others (2012). [2013] 117 CLA 227 (CLB).

Moore v. Regents of University of California (1990). 793 P.2d 479 (Cal. 1990).

Morrison v Moat (1851). (1851) 9 Hare 241.

Morse v Royal (1806). (1806) 12 Wes. 372.

N. Narayanan v. Adjudicating Officer, SEBI (2013). AIR 2013 SC 3191.

Nanalal Zaver and Ors. v. Bombay Life Assurance Co. Ltd. and Ors. (1950). AIR 1950 SC 172.

Narayan Bhagwantrao v. Gopal (1960). AIR 1960 SC 100.

Narayandas Shreeram Somani v. The Sangli Bank Ltd. (1965). AIR 1966 SC 170.

Naresh Trehan vs. Rakesh Kumar Gupta (2014). WP (C) No. 85/2010, Delhi High Court.

Needle Industries (India) Ltd. and Ors. v. Needle Industries Newey (India) Holding Ltd. and Ors. (1981). [1981] 3 SCR 698.

New York State Senate (2019). *Senate Bill S5642, 2019-20 legislative session.* New York State Senate. URL: https://www.nysenate.gov/legislation/bills/2019/s5642.

Nizam's Institute of Medical Sciences v. Prasanth S. Dhananka (2009). (2009) 6 SCC 1.

Norberg v. Wynrib (1979). (1979) 92 DLR 4th 449.

North, Michael (2002). *Greek medicine.* URL: https://www.nlm.nih.gov/hmd/greek/greek_oath.html.

Nosworth, Beth (2016). *A Director's Fiduciary Duty of Disclosure: The Case(s) Against.* URL: http://classic.austlii.edu.au/au/journals/UNSWLawJl/2016/51.html.

P Kishore Kumar and Ors. v. The State of Andhra Pradesh and Ors. (2016). W.P. Nos. 26929, 31164, 3138, 32264, 32591, 32760 of 2016, Andhra Pradesh High Court.

Parsa-Parsi, Ramin Walter (2017). *The Revised Declaration of Geneva: A Modern-Day Physician's Pledge.* URL: https://jamanetwork.com/journals/jama/fullarticle/2658261.

Pasqual, Frank (2017). *Towards a fourth law of robotics: Preserving attribution, responsibility and explainability in an algorithmic society.* URL: http://tiny.cc/ebp4az.

Patel, Nilay (2019). *Facebook's USD 5 billion FTC Fine is an Embarassing Joke.* URL: https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke.

Payne v. Evans (1874). [1874] 18 Eq 356.

Pearce v. United Bristol Healthcare NHS Trust (1998). 1998 (48) BMLR 118.

Punia, Swati, Amol Kulkarni, and Sidharth Narayan (2019). *User's perspectives on privacy and data protection.* URL: http://www.cuts-ccier.org/cdpp/pdf/survey_analysis-dataprivacy.pdf.

Puttaswamy v. Union of India (2017). 2017 (10) SCC 1.

Radhabari Tea Co Pvt. Ltd. vs. Mridul Kumar Bhattacharjee and Ors. (2009). [2010] 100 SCL 239 (Gau).

Raju Sebastian and Ors. v. Union of India and Ors. (2019). WA No. 2112 of 2018.

Ram Parshotam Mittal and Ors. v. Hotel Queen Road Pvt. Ltd. and Ors. (2019). 2019 (7) SCALE 738.

Ramaiya, A (2014). *Guide to the Companies Act (providing guidance on the companies act, 2013).* Ed. by Arvind Datar and S Balasubramanian. 18th ed. LexisNexis.

Re C (Adult: Refusal of Medical Treatment) (1994). [1994] 1 All ER 819.

Reibl v. Hughes (1980). (1980) 114 DLR (3d.)

Reserve Bank of India v. Jayantilal N Mistry (2015). TC (C) 91/2015, Supreme Court.

Rogers v. Whittaker (1992). 1992 (109) ALR 625.

Ropek, Lucas (2019). *NY?s Data Privacy Bill Failed: Is There Hope Next Session?* URL: https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html.

Rotman, Leonard I (2011). *Fiduciary Law's "Holy Grail": Reconciling theory and practice in fiduciary jurisprudence.* URL: http://tiny.cc/85g4az.

Sameer Kumar v. State of Uttar Pradesh (2014). 2014 Indlaw All 2804.

Schloendorff v. Society of New York Hospital (1914). 105 NE 92 (1914).

Schneir, Bruce (2009). *Its time to drop the 'expectation of privacy' test.* URL: https://www.wired.com/2009/03/its-timeto-drop-the-expectation-of-privacy-test/.

Secretary General, Supreme Court of India v. Subhash Chandra Agarwal (2010). AIR 2012 Del. 159.

Sengupta, Arghya (2018). *Why the Srikrishna Committee Rejected Ownership of Data in Favour of Fiduciary Duty.* URL: https://thewire.in/tech/why-the-srikrishna-committee-rejected-ownership-of-data-in-favour-of-fiduciary-duty.

Shri Rakesh Kumar Gupta vs. The Central Public Information Officer and The Appellate Authority, Director of Income Tax (Intelligence) (2011). CIC/DS/A/2011/001128, CIC.

Sidway v. Bethlem Royal Hospital Governors (1985). [1985] A.C. 871 (H.L.)

Sitkoff, Robert H (2014). "An Economic Theory of Fiduciary Law". In: *Philosophical Foundations of Fiduciary Law.* Ed. by Andrew S Gold and Paul B Miller. Oxford: Oxford University Press.

Smith v. Van Gorkem (1985). 488 A.2d 858.

Smt. Bina Barua and Ors. v. Dalowjan Tea Co. (P.) Ltd. and Ors. (1981). (1981) 1 GLR 55.

Spring Meadows Hospital v. Harjot Ahluwalia (1998). (1998) 4 SCC 39.

Swaminatha Aiyar v. Jumbukeswaraswami (1930). AIR 1930 Mad 372.

The Institute of Chartered Accountants of India v. Shaunak H Satya and Ors. (2011). AIR 2011 SC 3336.

Tiku, Nitasha (2019). *The EU Hits Google With a Third Billion-Dollar Fine. So What?* URL: https://www.wired.com/story/eu-hits-google-third-billion-dollar-fine-so-what/.

Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors. (2010). ILR 2010 (3) Ker 892.

Tsosie, Rebecca (2003). "The conflict between the public trust and the indian trust doctrines: federal land policy and native nations". In: *Tulsa Law Review* 39.2. URL: http://tiny.cc/wkw8az.

Turner v. Corney (1841). [1841] 5 Beav 517.

Union of India and Ors. v. VK Shad and Ors. (2012). 194 (2012) DLT 586.

Union of India v. Central Information Commission (2009). WP (C) No. 8396/2009, Delhi High Court.

Vaidhyanathan, Siva (2019). *Billion Dollar Fines Can't Stop Facebook and Google. That's Peanuts for Them.* URL: https://www.theguardian.com/commentisfree/2019/jul/26/google-facebook-regulation-ftc-settlement.

Whittaker, Zack (2018). *UK data protection complaints more than double under new GDPR rules.* URL: https://techcrunch.com/2018/08/28/uk-data-protection-complaints-spike-under-new-gdpr-rules/.

Williams, Richard (2012). *Enlightened Shareholder Value in UK Company Law.* URL: https://www.austlii.edu.au/au/journals/UNSWLawJl/2012/15.pdf.

Wynen, Anne Van Thomas (1949). "Note on the origin of uses and trusts - waqfs". In: *SMU Law Review* 3.2. URL: http://tiny.cc/6a75az.

Yannella, Philip N (2019). *New York State Data Privacy Law Fails.* URL: https://www.natlawreview.com/article/new-york-state-data-privacy-law-fails.

Acknowledgements

The authors thank Anirudh Burman, Pratik Datta, Smriti Parsheera, Renuka Sane and Faiza Rahman for comments. All errors are their own.

About the Authors

The authors are technology policy researchers at the National Institute of Public Finance and Policy (NIPFP), New Delhi.

datagovernance.org dgn@idfcinstitute.org

@datagovnetwork /datagovnetwork /datagovnetwork