DGN Policy Brief 04
January 2020

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

The Personal Data Protection Bill, 2018 (PDP Bill) uses the concept of a fiduciary relationship to protect personal data of individuals. However, this requires significant stretching of the concept to enable its use as a generic data protection framework. While the PDP Bill does cast various obligations on entities that could be seen as being similar to the duties in a fiduciary relationship, the standards of loyalty required by the draft law are extremely low, there being no requirement for the data fiduciary to act in the interests of or for the benefit of the data subject. Overall, the fiduciary framing in the draft law appears largely cosmetic. The law does not deem data processing entities to be fiduciaries, and further does not implement any particularly novel rights or obligations that draw from the fiduciary concept.

1. Introduction

Typically, a fiduciary relationship is one where a party holds a legal or ethical relationship of trust with another. Recent literature has attempted to introduce the concept to the growing 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 attractive in that it establishes a duty of care on those processing personal data, making it incumbent on them to act in the individual's interest. Nevertheless, the concept has 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 monetisation of user data).

The Justice Srikrishna Committee Report of August 2018 (the "Report") introduces the concept of a fiduciary relationship into privacy jurisprudence in India by attempting to categorise data processing entities as "data fiduciaries" and individuals as "data principals". The PDP Bill (the "PDP Bill") accompanying the Report attempts to operationalise the concept by establishing various rights of data principals and associated obligations on data fiduciaries.

The idea of using the fiduciary concept to protect an individual's privacy rights is not new - traditional fiduciary relationships such as that between a doctor and patient or a lawyer and client, do recognise duties of confidentiality. However, the PDP Bill is one of the first attempts to use the fiduciary framing as a basis for a generic data protection law.

In this context we examine:

- Whether all data processing entities are in fiduciary relationships with individuals (and therefore whether the fiduciary concept works as the basis for a generic data protection law)?
- Whether the use of the fiduciary concept can adequately protect an individual's privacy rights?
- Whether the obligations imposed by the PDP Bill are similar to the duties expected of traditional fiduciaries?
- Whether the fiduciary framing in the PDP Bill has any practical effect?

2. Understanding Fiduciary Relationships

There are numerous situations where we are required to place faith in a second party in order to achieve an end that is recognised as being in the broader social interest. The need for delegation however creates an agency

problem - the agent may act in its self interest (Sitkoff, 2014). In certain relationships legal protections stemming from contractual and tortuous obligations may not prove sufficient to safeguard the party's interests (Frankel, 1983) and (Rot- man, 2011, 3).[1]

The law therefore recognises a special class of relationships where there is a high degree of vulnerability between the parties, despite which one party is required to impose trust and confidence in the other (Miller, 2014) and (Rotman, 2011, 3). Whether a relationship is fiduciary or not is determined by examining the degree of dependence and vulnerability in the relationship, the expectation of trust, and the social value of the relationship (Rotman, 2011, 3). Generally speaking, the fiduciary must have the ability to unilaterally exercise discretionary power granted by the beneficiary, such that the beneficiary is peculiarly vulnerable to or at the mercy of the fiduciary (Frankel, 1983), (Miller, 2014) and (Treesa Irish w/o Milton Lopez v. Central In- formation Commission and Ors., 2010). The law recognises numerous relationships as having a fiduciary nature with some of the more commonly quoted examples in India law including trustees and beneficiaries, doctors and patients, guardians and wards, etc.

By recognising a relationship as having a fiduciary character, the law casts a series of onerous, principle based obligations on the more powerful party in the relationship. The most important duties in a fiduciary relationship are the duties of loyalty and care (Frankel, 2011). These imply that the fiduciary is required to:

• ensure that it acts so as to protect or advance the interests of the beneficiary (or to act for the benefit of the beneficiary) (Central Board of Secondary Education and Anr. v. Aditya Bandopadhyay and Ors., 2011), (Reserve Bank of India v. Jayantilal N Mistry, 2015), (Treesa Irish w/o Milton Lopez v. Central Information Commission and Ors., 2010). The fiduciary cannot normally put itself in a position that may be seen as conflicting with the interests of the beneficiary.[2]

• put in reasonable skill and diligence while handling the affairs of the beneficiary.

The exact formulation of these duties varies depending on the nature of the relationship at hand and the vulnerabilities therein. Being based in equity, there is no single standard of fiduciary law as such - though there are certain basic principles running through the various relation- ships deemed as fiduciary (Industrial Development Consultants v. Cooley, 1972), (Frankel, 1983), (Rotman, 2011, 3) and (Langbein, 2005). To illustrate, one may consider how the duty of loyalty has been interpreted in the context of trustee-beneficiary relationships and in the context of companies and their directors.

Trust law places a very high duty of loyalty on trustees. For example, the Trusts Act, 1882, recognises that trustees do not generally occupy an office of profit and places a series of prohibitions on self-dealing by the fiduciary. In many situations, even consent of the beneficiary is insufficient for the trustee to act in a manner considered detrimental to the beneficiary's interests. For instance, Section 53 of the Trusts Act permits the trustee to purchase the interest of a beneficiary only once a court is satisfied that the transaction is "manifestly to the advantage" of the beneficiary.

Company law too places duties of loyalty on directors, not- ably in Sections 166(2), (4) and (5) of the Companies Act, 2013. Generally speaking, directors are required to avoid any conflict of interest with the company whatsoever and cannot act to enrich themselves at the cost of the company. However, directors are permitted to engage in conflicting activities subject to sufficient disclosures being made to the company. Directors are, generally speaking, expected to act in a bona fide manner i.e. in good faith towards the company.

From our analysis, it appears that the degree of loyalty expected of a fiduciary is largely dependent on the nature/degree of the vulnerability and expectation of trust in a relationship (though the beneficiary's interests must al- ways be placed before that of the fiduciary). For instance, trust law appears to cast more onerous duties and limits the fiduciary's powers in more ways than company law. Often beneficiary's in a trust relationship will not have any ability to comprehend risks or

give proper consent (as may be the case where the beneficiary is a minor). In the company law context however the law recognises that if sufficient disclosures are made, shareholders and other stakeholders can act to protect the company against the erring director.

Apart from duties of loyalty and care, fiduciary relationships contain a range of subsidiary duties that largely seek to reduce information asymmetries, while also limiting the ability of the fiduciary to act outside the bounds of what is expected by the beneficiary.

3. Using the Fiduciary Concept to Protect Privacy Rights

While Indian law has had occasion to deal with the concept of confidentiality of information in the context of fiduciary relationships (notably under the Right to Information Act, 2005), the Report relies on writing by an American constitutional law expert - Jack Balkin - as a basis for using the fiduciary concept to protect personal data.

Balkin, in a series of articles and blogs, suggests that large data processing entities (such as social media companies) voluntarily comply with a series of privacy enhancing obligations, that would ensure they act in accordance with the expectations of their users. In exchange for adherence to these duties, service providers would receive immunity from prosecution under state or federal privacy laws (J. Balkin, 2014), (J. M. Balkin, 2016, 4)(J. M. Balkin & Zittrain, 2016).

Balkin's thesis is primarily motivated by two factors: first, the huge power differential between data processing entities and individuals caused due to the information asymmetries in the relationship (and the failure of the notice and consent model to adequately overcome this), and second, the primacy accorded to speech rights in the American constitutional arrangement, under which a comprehensive federal privacy law is likely to be held unconstitutional (J. M. Balkin, 2016, 4).

Balkin therefore suggest a number of possible duties of "in- formation fiduciaries", which are similar to duties cast on traditional fiduciaries in that they seek to ensure the data processing entity acts in a fair and reasonable manner and in accordance with the expectations of the individual (J. M. Balkin, 2016, 4) and (Dobkin, 2018).

In order to preserve the ability of service providers to monetise personal data, Balkin suggests adoption of a fairly low standard of loyalty for 'information fiduciaries' (J. M. Balkin, 2016, 4). This standard has however been criticised as distorting the fiduciary concept beyond recognition (Khan & Pozen, 2019). Balkin proposes adopting a "good faith" based standard, as opposed to a 'best interests' or a 'benefit of beneficiary' based framing as is traditionally seen in fiduciary relationships.[3]

The discussion above raises two questions: (a) can all or even any of the entities that process personal data be considered fiduciaries? (b) are fiduciary duties sufficient to protect privacy rights of users?

3.1. Are Data Processing Entities in Fiduciary Relationships With Their Users?

Balkin does not extend his thesis to all data processing entities. He suggests only covering those relationships where there is a special vulnerability created, or where the service provider attempts to induce trust of the user (J. M. Balkin, 2016, 4). This broadly corresponds with the Indian law on the issue (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).

The theory as expounded by Balkin is fairly narrow which could be seen as detracting from the use of the concept as a general data protection law. Many relationships of information exchange that would not qualify as fiduciary could nevertheless require some form of regulation (how- ever light-touch) in order to protect individual autonomy and privacy. Notably, the General Data Protection Regulation (GDPR) also extends to processing of personal data by individuals in certain contexts.

On the other hand, Indian courts have allowed separation of fiduciary parts of a relationship from other parts thereof (Union of India v. Central Information Commission, 2009) and (Canbank

Financial Services Ltd. v. Custodian and Ors., 2004). 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. That said, Indian courts have also held that relationships where there is no significant power differential are not fiduciary despite the exchange of confidential information, that relationships of service provision are not fiduciary in nature, and that situations where information is provided under a legal obligation are not covered under fiduciary relationships.[4] This appears to indicate that the use of a fiduciary framing may not be suitable to cover the breadth of situations that a generic data protection law may need to cover.[5]

In addition to issues concerning the breadth of the concept, commentators have also pointed to the dissonance in treating service providers as fiduciaries at all. This is on grounds that the business models of service providers, being based on monetizing user data, can never be squared with the fiduciary concept, which involves the fiduciary placing its interests second to that of the beneficiary (Khan & Pozen, 2019).

While undoubtedly true that fiduciary law requires the interests of the beneficiary to be given precedence over that of the fiduciary, it is worth noting that fiduciary law does recognise multiple standards of the duty of loyalty -based on the asymmetry or vulnerability at hand, the nature of the relationship, the ability of the beneficiary to understand the risks involved, and so on. It does not therefore appear in- conceivable for the concept to be made workable. A best interest or benefit based framing of obligations could in-deed force service providers to change some existing business models while not necessarily leading to a complete bar on targeted advertising or monetisation of user data.

Overall, it appears that data processing entities can certainly be in a position of power with respect to users by virtue of the information that users have to provide to them. 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 (Punia, Kulkarni & Narayan, 2019). 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 relation- ships, 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 (whether such a relationship should continue to be called fiduciary is an- other matter). Duties can then be imposed that are similar to those in a fiduciary relationship should this be felt necessary to solve a particular social problem.

3.2. Does the Concept Ensure Adequate Rights Protections?

While the breadth of the information fiduciary 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[6] or in- deed the scope of the data that forms the basis for the relationship.[7] The imposition of a high duty of loyalty and care for instance, could lead to a high standard of rights protection by ensuring that data processing entities can only use data for the benefit or to maximise the gains to the individual concerned. The use of the fiduciary concept could also mean that obligations will be imposed irrespective of contractual terms between the parties. The duty

of care requirement in a fiduciary relationship could be interpreted to imply security and other related obligations on data processing entities.

Despite the largely positive response the 'information fiduciary' concept has received, there remain questions as to the efficacy of the concept in protecting privacy rights.

First, it has been 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 & Pozen, 2019). While existing law does indeed give consumers some remedies against privacy invasive practices, 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 ex- press "good faith" requirement as US law does[8]. 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.

Second, the information fiduciary concept applies to in- formation 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 use of this concept lacks any independent normative standard and therefore does not adequately protect privacy rights (Crowther, 2012) and (Schneir, 2009). Balkin himself notes that the standard he proposes would require users to factor the monetisation of their data into account (J. M. Balkin, 2016, 4). This may not be possible for all users. Expectation and reasonable- ness based standards are also said to disproportionately impact vulnerable sections of the populace, who may in fact require stronger privacy protections (Gellman & Adler- Bell, 2017).

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.

Third, concerns about the workability of the notice-consent framework as a means to overcome information asymmetry issues remain. As Khan and Pozen point out, the nature of information asymmetry in the digital ecosystem is of a significant order (Khan & Pozen, 2019). 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.

However, as described previously, the fiduciary concept does indeed allow for strong protections to be implemented, as is the case with the two draft American laws being considered in New York and at the federal level. Notably, these laws specifically deem data processing entities as fiduciaries thereby requiring them to place their user's interests ahead of their own, and avoid acting in a manner that could be considered unexpected or offensive to a reasonable user.

4. Examining the Fiduciary Concept in the PDP Bill

The Report chooses to utilise the fiduciary framing as the basis for the PDP Bill in view of the perceived vulnerability of users to data processing entities and the apparent ability of the concept to balance rights protection with business interests. The concept is said to preserve autonomy of individuals while still enabling rights protection. However, the Report 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, or in-
deed whether a generally recognised duty to act in the individual's interest exists in all relationships of information exchange.
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 typic- ally 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 hurdles, it makes sense to use the fiduciary framing if the concept would allow novel data protection related obligations to be imposed. As indicated previously, the fiduciary concept can indeed cast a high standard of obligations on entities brought under this framework (that can go beyond typic- ally seen data protection obligations). For instance, the two draft US laws mentioned above both cast specific and high standards of loyalty and care on data controllers. These re- strict 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 (New York State Senate, 2019).

However, a summary analysis of the PDP Bill with the GDPR indicates that the two laws are largely similar in terms of the nature of obligations imposed (though the ex- act scope/ contours of the obligations are different based on the specific language used in the laws). Both use largely notice and consent based models to protect user privacy (though this is enhanced and contains safeguards that are not normally present in contract law). Both regimes at- tempt to ensure individuals are informed of processing activities and that individuals are given control of their personal data not least through principles of purpose limitation, high standard of consent, detailed notice requirments, provisions aimed at reducing information asymmetry, etc.

4.1. Are the Duties Under the PDP Bill 'Fiduciary' Duties?

To eliminate or reduce the possibility of an abuse of power by a data fiduciary, the draft PDP Bill: (a) casts a generic obligation on all data fiduciaries to process personal data in a "fair and reasonable" manner; (b) lays out numerous specific measures that cast a duty of care on data fiduciaries (to process data in accordance with the expectations of the data principal). 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.

By requiring the data fiduciary to inform the data principal of relevant processing practices, by ensuring purpose limitation, 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. As mentioned previously, Indian law 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. "Predictability" of processing - which is what the draft law aims at - is not synonymous with processing in the data principal's interests of for its benefit. Though the Report 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 standard applied in the PDP Bill only requiring data fiduciaries to act in a bona fide, diligent and reasonable manner. Notably, the PDP Bill itself uses the phrase "best interest" only once - in the context of protection of children's data.

A lower standard is generally used where it is easier to overcome information asymmetry problems or where social norms otherwise dictate the need to do so (Langbein, 2005). Accordingly, the low standard used in the draft law can be traced to the Justice Srikrishna

Committee aiming to balance business and individual interests (as is done by Balkin). As indicated previously, 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 et al., 2019), (Bailey, Parsheera, Rahman & Sane, 2018) and (Matthan, 2017). On the other hand, by imposing such a standard, the law 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). Further, the safe-guard 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. However, relying on the data protection authority to ban pernicious practices is not the same as requiring the data fiduciary to act in the interests of or for the benefit of the data principal. Empower-ing 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.

While in traditional fiduciary relationships informed con- sent can be used to reduce/waive the obligations on the more powerful entity, the law also imposes various safe- guards 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 context of trusts, courts are permitted to step in and act in their interests. The draft law does not specifically circumscribe the ability of the individual to con-sent to activities that may not necessarily be in his or her interest. This is not per se against the fiduciary concept, though, both academics and courts appear to be hesitant
about recognising the entirety of a fiduciary relationship to be voluntary/subject to contractual waivers (Leslie, 2005) and (Union of India v. Central Information Commission, 2009). 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 in- formation 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.[9] The "informed consent" requirement in the draft PDP Bill places a high standard of consent, even more so than the standards recognised in Indian medical jurisprudence (v. Dr. Prabha Manchanda, 2008). Similar to the obligations imposed in traditional fiduciary relationships, the mechanisms used by the PDP Bill to ad- dress 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.

- *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 worldwide turnover of the violating entity.

Overall, it can be seen that the PDP Bill does indeed implement duties akin to that in traditional fiduciary relation- ships. The duties in the draft law 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. One may question whether the standard used in the draft law 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 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.

4.2. Effect of Using the Data Fiduciary Framing in the PDP Bill

The use of the term "data fiduciary" in the draft law does not in itself 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.[10] The entities that come within the definition in the law would be subject to the (fiduciary like) obligations provided in the PDP Bill itself but would not necessarily be required to adhere to the obligations or standards typically imposed on fiduciaries (for instance, under Section 88 of the Trusts Act).

The use of the phrase "data fiduciary" is largely meaning- less 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. The fiduciary concept is something that is used in many legal con- texts and is a term that people are familiar with (even if the nuances of this relationship are not very well under- stood). 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. The motivation for using the fiduciary concept could also be the need to differentiate the PDP Bill from laws such as the GDPR, particularly in view of the Srikrishna Committee's self-imposed mandate to find a "fourth path" to data protection.

5. Conclusion

The information fiduciary concept is an interesting method used 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 ap- pears 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. Notably, 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).

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). 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).

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 cur- rent 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 cast on fiduciaries, also implies that decisions regarding permitted practices will be made by executive authorities rather than adjudicatory authorities. These issues detract from the fiduciary character sought to be established by the draft law.

But the draft law does, to an extent, meet the aim of pre- serving 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.

However, the same ends could be achieved without using the fiduciary concept at all - as is done in the case of the GDPR. One may speculate that the use of the terminology could be necessitated by the need to differentiate the PDP Bill from the GDPR, or to take an uncharitable view, to make it appear that the law contains a higher standard of rights protection than it actually does.

Notes

1. This may occur for instance, in situations where the power differential between parties is so high that there is a limited possibility of fair contracting. Contract law would merely forbid such contracts or enable restoration of status quo post breach. Social interest may however require parties to enter into such relationships, without facing the possibility of adverse consequences (Frankel, 1983) and (Rotman, 2011, 3).

2. 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. (Sitkoff, 2014) and (Langbein, 2005).

3.This standard implies that parties must act reasonably, honestly, fairly, with due care and attention. Parties will be required 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). A 'best interest' or 'benefit' requirement on the other hand could imply that the service provider may be barred from profiting from personal data in any way at all, if at the expense of the user. Existing business models of online service providers could therefore be- come difficult to justify should such a standard be implemented, though rights protection would certainly be enhanced.

4. Refer to (Canbank Financial Services Ltd. v. Custodian and Ors., 2004), (Central Board of Secondary Education and Anr. v. Aditya Ban- dopadhyay and Ors., 2011), (Reserve Bank of India v. Jayantilal N Mistry, 2015), (Bihar Public Service Commission vs. Saiyed Hussain Abbas Rizwi and Ors., 2012), (Secretary General, Supreme Court of India v. Subhash Chandra Agarwal, 2010), (Naresh Trehan vs. Rakesh Kumar Gupta, 2014), and (Shri Rakesh Kumar Gupta vs. The Central Public Information Officer and The Appellate Authority, Director of Income Tax (Intelligence), 2011)

5. The fiduciary concept is largely used in circumstances where social interest requires one party to be protected against another due to the vulnerability between the two. The law therefore places an onus on the fiduciary to place the beneficiary's interests above its own. 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.

6. Balkin suggests some basic duties for information fiduciaries including to (a) institute a set of fair information practices (to set expectations of users and reduce information asymmetry), (b) disclose data breaches (to reduce information asymmetry), (c) 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), (d) agree not sell or distribute consumer information except to those who agreed to similar rules (to preserve duties of loyalty and care) (J. M. Balkin, 2016, 4). These duties are further expanded by (Dobkin, 2018). Using the test of whether a practice is acceptable or not, based on a user's expectations, she suggests four principles around which the du- ties of an information fiduciary could be framed - importantly recognising that the concept could lead to a bar on manipulation of users and discrimination using personal data.

7. 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 relation- ship, with an attendant expectation of confidentiality (i.e. the data should not be publicly known information). Therefore, the concept could also be used to cast obligations qua the usage of non-personal data gleaned from a user, as well as non-personal data derived from personal data of a user. This is in fact what is attempted in two draft American laws - New York's

Privacy Act and the federal Data Care Act.

8. Indian law only requires insurance contracts to be entered into in “utmost good faith”, which entails disclosure of all material facts (Makkar, 2018) and (Law Commission of India, 2006)

9. 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.

10. The two draft America laws mentioned previously do however contain deeming provisions, that recognise relevant data processing entities as fiduciaries and ascribe to them the various duties that come with a fiduciary relationship.

References

Bailey, R., Parsheera, S., Rahman, F. & Sane, R. (2018). Disclosures in privacy policies: Does notice and consent work? NIPFP Working Paper No. 246. Retrieved from https : / / www. nipfp . org . in / media / medialibrary / 2018/12/WP 246.pdf

Balkin, J. (2014). Information fiduciaries in the digital age. Retrieved from https://balkin.blogspot.com/2014/ 03/information-fiduciaries-in-digital-age.html

Balkin, J. M. (2016). Information fiduciaries and the first amendment. Retrieved from https://lawreview.law. ucdavis.edu/issues/49/4/Lecture/49-4 Balkin.pdf

Balkin, J. M. & Zittrain, J. (2016). Retrieved from https : / / www. theatlantic . com / technology / archive / 2016 / 10/information-fiduciary/502346/

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) 13 SCC 61.

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

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

Crowther, B. (2012). (un)reasonable expectation of digital privacy. BYU Law Review, 2012(1). Retrieved from http://tiny.cc/7ptabz

Dobkin, A. (2018). Information fiduciaries in practice: Data privacy and user expectations. Retrieved from http: / / btlj . org / data / articles2018 / vol33 / 33 1 / Dobkin Web.pdf

Frankel, T. (1983). Fiduciary law. Retrieved from https://scholarship.law.berkeley.edu/californialawreview/ vol71/iss3/1/

Frankel, T. (2011). Oxford University Press. Gellman, B. & Adler-Bell, S. (2017). The disparate impact of surveillance. Retrieved from http://tiny.cc/o5tabz Industrial Development Consultants v. Cooley. (1972).

[1972] 1 WLR 443.Khan, L. & Pozen, D. (2019). A skeptical view of information fiduciaries. Retrieved from http : // tiny . cc /hhim7y

Langbein, J. H. (2005). Questioning the trust law duty of loyalty: Sole interest or best interest? Yale Law Journal, 114(1). Retrieved from https : / / law . yale . edu / system / files / documents / pdf / Faculty / Langbein Questioning the Trust.pdf

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

Leslie, M. (2005). Trusting trustees: Fiduciary duties and the limits of default rules. Georgetown Law Journal, 94(1). Retrieved from http://tiny.cc/czthbz

Makkar, A. S. (2018). Doctrine of good faith and fair deal- ing: Lacuna in indian contract law. Retrieved from https : / / indiacorplaw. in / 2018 / 12 / doctrine - good - faith-fair-dealing-lacuna-indian-contract-law.html

Matthan, R. (2017). Beyond consent: A new paradigm for data protection. Retrieved from https:// takshashila. org.in/discussion-document-beyond-consent-new- paradigm-data-protection/

Miller, P. B. (2014). The fiduciary relationship. In A. S. Gold & P. B. Miller (Eds.), Philosophical foundations of fidu- ciary law. Oxford: Oxford University Press.

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

New York State Senate. (2019). Senate bill s5642, 2019-20 legislative session. New York State Senate. Retrieved from https://www.nysenate.gov/legislation/bills/ 2019/s5642

Punia, S., Kulkarni, A. & Narayan, S. (2019). User's per- spectives on privacy and data protection. Retrieved from http://www.cuts-ccier.org/cdpp/pdf/ survey analysis-dataprivacy.pdf

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

Rotman, L. I. (2011). Fiduciary law's "holy grail": Recon- ciling theory and practice in fiduciary jurisprudence. Retrieved from http://tiny.cc/85g4az

Schneir, B. (2009). Its time to drop the 'expectation of pri- vacy' test. Retrieved from 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.

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

Sitkoff, R. H. (2014). An economic theory of fiduciary law. In A. S. Gold & P. B. Miller (Eds.), Philosophical founda- tions of fiduciary law. Oxford: Oxford University Press.

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

Union of India v. Central Information Commission. (2009). WP (C) No. 8396/2009, Delhi High Court. v. Dr. Prabha Manchanda, S. K. (2008). (2008) 2 SCC 1.

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.

About the Authors

The authors are Fellows at the National Institute of Public Finance and Policy.

Acknowledgements

The authors thank Anirudh Burman, Pratik Datta, Smriti Parsheera, Renuka Sane, participants at the Data Governance Network meeting of September, 2019, and an unknown reviewer for comments. All errors are their own.

Disclaimer

The views and opinions expressed in this paper are those of the authors and do not necessarily represent those of the National Institute of Public Finance and Policy.

IDFC Institute
3rd Floor, Makhija Chambers, 196 Turner Road,
Bandra(W), Mumbai 400050

/idfcinstitute @idfcinstitute /IDFCInstitute