Protecting Privacy in India: The roles of consent and fairness in data protection

Mark J Taylor and Jeannie Marie Paterson***

Abstract *The Indian Personal Data Protection Bill 2019 provides a unique approach to balancing the elements of individual consent and fairness-based limitations that are used in data protection regimes in other parts of the world. Drawing on the fundamental values and interests recognised in KS Puttaswamy v. Union of India (2017) and the report of the Committee of Experts, the Bill requires consent of the data subject to data processing, and puts in place standards that consent must meet to be more than a forced formality. Its novelty lies in also proposing substantive obligations of fair and reasonable data processing, and by making organisations responsible, as statutory 'data fiduciaries', for complying with obligations protecting the interests of the data subject. The requirement that processing be fair, also written into European data protection law, is an opportunity to put data controllers under an obligation to protect the interests of data subjects. Data processing ought not to have a negative impact upon an individual's interests, values and freedoms disproportionate to their positive gains. If robustly interpreted and applied, this could be an effective protection against the shortcomings of consent as a safeguard for protecting individual interests. European data protection law has yet to fully embrace this opportunity. If it did, then there would be less pressure to ensure a data subject's consent meets ideal standards of 'free and informed', which is increasingly unrealistic in a modern information society. Considering the merits of these different approaches, with different degrees of relative emphasis upon individual consent and objective tests of fairness, prompts reflection upon the proper function of privacy and data protection legislation within society. Is it purely to enable individual expressions of informational self-determination — irrespective of whether the deal done is a good one? Or does data protection law also have a role in expressing community expectations by promoting norms and standards of fair dealing that are conducive to individual well-being and to civil society as a whole?*

* Associate Professor in Health Law and Regulation, Melbourne Law School, University of Melbourne, Australia.

** Professor, Melbourne Law School, University of Melbourne, Australia.

I. Introduction

Consent is widely used in data protection legislation as a mechanism for authorising use of personal and sensitive data. The significance and function of consent in such legislation can be understood in different ways. It may be understood to have a central role, perhaps *the* starring role: manifesting respect for informational self-determination and data sovereignty. Or, it may rather be understood to form part of an ensemble cast: existing within a broader complex of social norms and expectations; dictating when, and how, people ought to be asked about uses of information but not investing an individual with primary responsibility to safeguard their relevant interests. Of course, these might better describe points on a spectrum than binary opposites. The further toward the 'self-determination' end of the spectrum, then the greater the (neo-liberal) significance attached to individual autonomy and individual rights including potentially trumping social welfare goals. The further to the opposite end, then the more room there is to contextualise (or constrain) individual expressions of self-determination and to accommodate collective (or communitarian) interests. Both approaches require rules around what amounts to valid, as opposed to forced, consent and protections to ensure individuals are free from misrepresentation or coercion. However, we suggest that both approaches are strengthened from some role being given to measures for requiring 'fair' data processing. This requirement goes beyond consent as the primary safeguard for data protection and justifies the role of other broader considerations. These may be more overtly paternalistic,[1] limiting the types of data use consumers may consent to on grounds that they did not genuinely understand the potential risks in the use, or that the use was potentially harmful to them regardless.[2] It may also open up a

[1] 'The doctrine of paternalism justifies intervention by the state contrary to the wishes of the person whom that intervention is designed to benefit': Peter Cartwright, *Consumer Protection and the Criminal Law: Law, Theory, and Policy in the UK* (Cambridge University Press, 2001) 32.

[2] Adams and Brownsword note the paternalistic principle to be a feature of a consumer-welfarist ideology: 'contractors who enter into imprudent agreements may be relieved from

role for more public interest considerations, such as furthering public goods or protecting groups or society, incurred by individuals' present decisions.

We do not need here to determine which of these is the correct approach, or if there is indeed *a* correct approach. We outline the alternatives only to draw attention to some ambivalence within existing privacy and data protection law with regards to the function of consent relative to achievement of the purposes of privacy and data protection. This ambivalence can be seen in *KS Puttaswamy* v. *Union of India* (2017) ('*Puttaswamy*').[3] Here the Supreme Court of India recognised a right to privacy inherent to the constitutional right to liberty to be motivated by an imperative to assure the dignity of the individual.[4] The relationship between privacy, liberty, and a respect for human dignity can, however, be configured in different ways; with different implications for the relevance of individual consent. What is the conceptual connection between privacy and autonomy? Is data protection concerned with privacy or more discrete goals such as security or providing protection to individuals in circumstances where there is a significant imbalance of bargaining power? What is the significance of social norms or collective interests to the protection of human dignity? Answers to these questions are needed to properly contextualise the meaning and function of individual consent within a privacy or data protection regime. However, clear answers are rarely forthcoming.

Despite the ambiguity, the Indian Supreme Court in the *Aadhaar-5 Judge* decision[5] found the constitutionally protected privacy interest to be sufficiently certain to strike down elements of the Aadhaar scheme. The Court found that a compelling public interest might place a reasonable limit on privacy, but some parts of the scheme failed to meet this standard. As a consequence, *irrespective of any consent*, it was not permissible for individuals to contract with private individuals or corporations to enable them to seek authentication via the scheme.[6] Individuals were thus protected from making

---

their bargains where justice so requires. The case for paternalistic relief is at its most compelling where the party is weak or naïve': John N Adams and Roger Brownsword, 'The Ideologies of Contract' (1987) 7(2) *Legal Studies* 205, 212.

3 *KS Puttaswamy v Union of India* (2017) 10 SCC 1 ('*Puttaswamy*').

4 'Dignity is the core which unites the fundamental rights because the fundamental rights seek to achieve for each individual the dignity of existence. Privacy with its attendant values assures dignity to the individual and it is only when life can be enjoyed with dignity can liberty be of true substance. Privacy ensures the fulfilment of dignity and is a core value which the protection of life and liberty is intended to achieve': ibid [107]. See also, in particular, [113], [169].

5 *KS Puttaswamy v Union of India* (2019) 1 SCC 1 ('*Aadhaar-5 Judge*').

6 For further challenge on constitutional grounds see <https://www.hindustantimes.com/india-news/sc-to-hear-pleas-challenging-aadhaar-verdict-on-june-9/story-F0fzhuen7DIhtbhIijNlzM.html>.

bargains perceived to represent an unjustified and disproportionate privacy interference. This position has been changed through statutory reform now to allow voluntary use by private entities.[7] The point thus underlined: there is contestation over the extent to which an individual's ability to consent to uses of data that are objectively perceived to be unfair is to be limited.

These themes were comprehensively explored in the subsequent Report of the Committee of Experts, under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, submitted to the Ministry of Electronics and Information Technology, Government of India in 2018. This report took as threshold premise that, first, 'the primary value that any data protection framework serves must be that of privacy' and second, 'such a framework must not overlook other values including collective values'.[8] The Committee recommended that consent in this framework should be made meaningful through form and substance requirements imposed on entities seeking consent.[9] In addition, to protect data subjects, substantive obligations to ensure fair and reasonable data processing should be imposed on data controllers, who should be termed 'data fiduciaries'.[10] This protectionist approach is largely implemented in the proposed Indian *Personal Data Protection Bill 2019*.[11] The Bill adopts a substantive standard of 'fair and reasonable' that appears to go beyond that previously seen in data protection legislation as well as adopting the nomenclature of the data fiduciary.

In this article we reflect on the approach taken in the Indian *Personal Data Protection Bill 2019* and the insights it might offer for an understanding of 'fair' processing in other data protection legislation. We consider the potential for a 'fair' processing requirement, particularly when combined with the idea of a data controller as a statutory 'fiduciary', to supplement, and in some cases overtake, even the most robust requirements for a valid consent to data processing. Specifically, we suggest that if operating successfully, a requirement for 'fair' processing may mitigate the need for the

---

7 The Aadhaar and Other Laws (Amendment) Act 2019. For commentary: see 'Lok Sabha Passes Aadhaar Amendment Bill', *The Economic Times* (online, 4 July 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/lok-sabha-passes-aadhaar-amendment-bill/articleshow/70078736.cms>.

8 Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Report to Ministry of Electronics and Information Technology, Government of India, 27 July 2018) 10 ('*Protecting Privacy, Empowering Indians*').

9 ibid 11.

10 ibid 33.

11 Personal Data Protection Bill 2019 (India) <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>.

high threshold for valid consent now set by European data protection law: a substantive restriction on unfair processing might complement, rather than conflict with, consent requirements in ways that allow the standards of valid consent to be less demanding.

In our view, privacy and data protection legislation in Europe can sometimes appear internally conflicted between what might be described as 'market individualist' or 'consumer welfarist' modes, which correlate with the spectrum opposites in approaches to data protection we discussed earlier.[12] A 'market individualist' approach is guided by an ideological commitment to idea that the market place is a site for *competitive* exchange and that individual self-determination is to be respected with minimum judicial intervention. A 'consumer welfarist' approach, on the other hand, will tend to support more interventionist policy. According to Adams and Brownsword,

> [t]he consumer-welfarist ideology stands for a policy of consumer protection, and for the principles of fairness and reasonableness in contract. It does not start with the market-individualist premise that all contracts should be minimally regulated. Rather it presupposes that consumer contracts are to be closely regulated.[13]

While concerned with more than contracts and reasonable consumer expectations, European data protection law displays at times the hallmarks of an individualist mindset. It relies on a robust standard of affirmation, more robust even than that required under contract law, and an individual can choose to accept certain risks with regard to data processing so long as that high threshold of consent is satisfied. At other times, it seems more closely aligned with a consumer welfarist or communitarian mindset. It does, after all, explicitly require that processing must be 'fair', as well as lawful. And, lawful processing does not require consent. It is not even 'first amongst equals' when establishing a legal basis for processing, with various individual and collective safeguards inbuilt to alternatives.

Our argument is that, perhaps ironically, the direction of travel proposed under the *Consumer Data Protection Bill 2019* may be beneficial whether the intent is to support a 'market individualist' *or* a 'consumer welfarist' approach. Placing central reliance on consent can be problematic whichever end of the spectrum you are seeking to support. If consent is the principal

---

[12] For the framing of the values see Roger Brownsword, *Contract Law: Themes for the Twenty-First Century* (2nd edn, OUP 2006) 105–8; Roger Brownsword, 'Individualism, Cooperativism and an Ethic for European Contract Law' (2001) 64(4) *Modern Law Review* 628, 630.

[13] Adams and Brownsword (n 2) 205–23.

safeguard, and the aim is to enable informational self-determination, then the tendency will be toward insisting upon a very high standard for valid consent. We have seen this move within European data protection law under the *General Consumer Data Protection Right* ('*GDPR*').[14] However, the risk is that this provides little real protection to data subjects in advancing and protecting autonomy in practice. This might be because data subjects fail to exercise the right to control uses of their data as intended by the legislation. They may, for example, be overloaded by information or suffer consent fatigue.[15] The role of consent in protecting data subjects may also be undermined by data controllers choosing the other pathways for data use in preference to the arduous requirements for collecting consent. It is equally clear that a central reliance upon consent may fail to support a 'welfarist' position, given poor decisions will be allowed to stand regardless of consequences and genuinely beneficial social welfare may be overlooked. The result is that, whether minded toward an 'individualist' or 'welfarist' position, there may be good reason to support contextualising a (more modest) consent standard and, simultaneously, imposing substantive standards of fairness on personal data processing.

The proposed data protection legislation in India contemplates substantive limits being imposed on data processing even where consent is obtained. These limits are imposed through the use of a concept of a data fiduciary, who is under an obligation to only process data where this is fair and reasonable in the circumstances. Such an approach may be seen as paternalistic because it may, in some circumstances, override consent. However, it offers the potential, we suggest, for advancing broader goals. We suggest that mechanisms for promoting substantive standards of fair data protection — the aim of the fiduciary model — can be used to both protect individual data subjects and to advance collective welfare, wherever the ideal balance may be sought. At least in the UK, the fairness qualification on data processing under European data protection law has largely been applied to require procedural requirements of transparency rather than substantive protections on the interests of the data subject. If the limits on consent as a safeguard are not genuinely addressed, then this promotes neither a welfarist nor individualist agenda.

---

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1< https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> ('*GDPR*').

[15] See also Damian Clifford and Jeannie Marie Paterson, 'Consumer Privacy and Consent: Reform in the Light of Contract and Consumer Protection Law' (2020) *Australian Law Journal* (forthcoming).

We are candid that our view is that there may be significant advantages in a modern information society to adopting a relatively clear 'welfarist' position: with protections not only built into the limits of informational self-determination but into a responsibility on data controllers to act in the best interests of data subjects. As with welfarist positions in contract law, it places less emphasis on a 'gold-plated' consent and instead establishes the effective controls beyond consent. However, our argument is that this recognition of the role for standard-based limitations of fairness on data processing might also be advantageous if you prefer an individualist perspective. The paradox of leaning too heavily on consent as a safeguard is that such reliance may simply overburden that concept. The effect of bounded rationality on individuals' decision-making capacity may mean they do not benefit from the extensive requirements in data protection legislation for obtaining consent. Moreover, these requirements can raise the threshold for valid consent to a point that organisations consider unattainable; thereby encouraging them to rely upon alternatives. Establishing a 'valid' consent is just too hard, and the conditions for even individual control may be diminished.

Given the exponential growth in new technologies in providing both public and private sector services to consumers and citizens, concerns over data protection and privacy are likely to continue to assume prominence in public policy debate and law reform. Like the Court in *Aadhaar*, we are particularly interested in ensuring protections that are adequate to an information age, characterised by novel methods of data mining, machine learning, and ever-expanding big data. The Report of the Committee of Experts on Data Collection and Privacy, as well as the Bill that followed it, make clear that consent-based mechanisms are necessary but not sufficient at this time in history, and that there are compelling reasons to provide protections beyond consent in both promoting individual rights around privacy and collective, welfarist goals.

II. Privacy, Liberty and Human Dignity in Indian Privacy Reform

A. The Decisions in Puttaswamy and Aadhaar

In 2016 the Indian government introduced the Aadhaar scheme, under which demographic and biometric data of individuals is compiled by the government through the Unique Identification Authority of India ('UIDAI'). The UIDAI associates the demographic and biometric data with a 12-digit unique identity number (called 'Aadhaar'). This number is used to access a

number of different government services. There were also demands for it to be used to access commercially provided services.[16] The *Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act* 2016 ('*Aadhaar Act*') governing the uses of the biometric identifier was questioned on the ground that it violated a constitutionally guaranteed right to privacy (under Article 21). Before the question of whether the Aadhaar scheme violated a right to privacy could be properly addressed, it had first to be determined whether the Indian Constitution guaranteed such a right. Previous caselaw had indicated otherwise.

In order to determine whether the Indian Constitution protected a right to privacy, and to address the fact that an eight bench court in *MP Sharma* v. *Satish Chandra* and a six bench court in *Kharak Singh* v. *State of UP* had indicated that it did not, the Supreme Court assembled a nine bench court to consider the question in *Puttaswamy*.[17] The Supreme Court in *Puttaswamy* decided that privacy is a constitutionally protected right. This emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution and other provisions under fundamental rights contained in Part III.

The nature of the interest protected, and its relationship with liberty and other concepts — such as human dignity — was articulated in a variety of ways by the Court. The significance of self-determination may be understood to resolve differently according to whether emphasis is upon privacy as emergent from a right to liberty (guaranteed by Article 21) or privacy as a facet of human dignity (guaranteed by the fundamental rights contained in Part III of the Constitution). The right to liberty may be varyingly conceived to permit interference necessary to protect long-term freedoms and reciprocal duties to others. Human dignity itself might be resolved as a motivation for *empowerment* or *constraint*.[18]

If sympathy tends toward ideas of individual liberty and human dignity as empowerment at one end of the spectrum, then a respect for human dignity may support relatively untrammelled respect for autonomy and self-determination. The court favourably quoted Aharon Barak (former Chief Justice of the Supreme Court of Israel):

---

[16] There was media reporting of private firms previously asking customers to 'mandatorily link Aadhaar': Anonymous, 'Sec 57 of Aadhaar Act Struck Down. Here's What it Means for You', *The Quint* (online, 26 September 2018) <https://www.thequint.com/news/india/supreme-court-strikes-down-section-57-of-aadhaar-act-what-it-means-for-you>.

[17] (2017) 10 SCC 1.

[18] Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (OUP 2001).

> The best decisions on how life should be lived are entrusted to the individual. They are continuously shaped by the social milieu in which individuals exist. The duty of the state is to safeguard the ability to take decisions — the autonomy of the individual — and not to dictate those decisions.[19]

If sympathy tends toward maintaining the conditions capable of affording freedom and liberty for all members of society across the long-term, or human dignity as constraint, then one might not so readily entrust decisions on data flows to individuals operating under conditions of bounded rationality.[20] Specific choices may be denied to an individual if inconsistent with enduring autonomy or a particular idea of a dignified life[21] or the values of society. That respect for human dignity affords limited individual freedom is reflected in the view that the entitlements to be protected are foundational to social order. This view was also expressed in *Puttaswamy*:

> At a descriptive level, privacy postulates a bundle of entitlements which lie at the foundation of ordered liberty.[22]

The decision, therefore, shows ambivalence about the extent to which self-determination, or at least informational self-determination, should prevail over judicially dictated reasonable expectations regarding information norms. The latter leaves open still a wide range of views of what constitutes a properly ordered society: what 'fair' means.

---

[19] *Puttaswamy*, [105].

[20] On the inferences for consumer protection drawn from the reality of the bounded rationality of consumers: see further Geraint Howells, 'The Potential and Limits of Consumer Empowerment by Information' (2005) 32(3) *Journal of Law and Society* 349, 358–9.

[21] This is consistent with what Beyleveld and Brownsword describe as 'human dignity as constraint': Beyleveld and Brownsword (n 18). This view is also expressed by some theorists that respect for human dignity may require some autonomous choices (e.g. to clone a human being) to be restricted: see, e.g., Leon R Kass, *Life, Liberty and the Defense of Dignity* (Encounter Books, 2002); Francis Fukuyama, *Our Posthuman Future: Consequences of the Biotechnology Revolution* (Picador, 2003).

[22] *Puttaswamy*, [185]. This idea is picked up in the later case of *Cochin Institute of Science & Technology v Jisin Jijo* 2019 SCC OnLine Ker 1800, [298]–[299]: 'the notion that there must exist a reasonable expectation of privacy ensures that while on the one hand, the individual has a protected zone of privacy, yet on the other, the exercise of individual choices is subject to the rights of others to lead orderly lives. For instance, an individual who possesses a plot of land may decide to build upon it subject to zoning regulations. If the building bye laws define the area upon which construction can be raised or the height of the boundary wall around the property, the right to privacy of the individual is conditioned by regulations designed to protect the interests of the community in planned spaces. Hence while the individual is entitled to a zone of privacy, its extent is based not only on the subjective expectation of the individual but on an objective principle which defines a reasonable expectation.'

When it came to applying the decision in *Puttaswamy* to the Aadhaar scheme, a five-judge bench in the Supreme Court[23] concluded that elements of the scheme did not meet the requirement that the right to privacy should be impinged only with a just, fair,[24] and reasonable law. The *Aadhaar* Court held that the Aadhaar scheme served an important social or public interest in general terms, and the constitutionality of the Act could be substantially upheld. The use of the biometric data for accessing government services was constitutional based on the proportionality principle. However, the Court also found it necessary to either strike down or read down elements of the *Aadhaar* scheme on the ground that they were incompatible with the constitutionally protected right to privacy. These included that retention of data beyond a period of six months is impermissible; regulation 27 of the *Aadhaar (Authentication) Regulations 2016* which provided for archiving for a period of five years was struck down. Also, section 57 which allowed for the scheme to be used for any purpose was read down to mean such a purpose as backed by law. The significance of this is that it denied the possibility that contract alone could be sufficient to establish a right to use the Aadhaar number for services such as banking, telecommunications or education.[25] Private organisations, and individuals, were thus denied the possibility of using the scheme to authenticate the identity of individuals; such use was considered a disproportionate interference with privacy.[26]

Since the judgment in *Puttaswamy* was handed down, there has been statutory reform that will now permit private entities to request and use the biometric Aadhaar data.[27] This itself reflects a difference of opinion on whether the use of the Aadhaar scheme by private bodies like telecom companies and banks is a use of personal information to which individuals should be entitled to agree. The welfarist approach of the Court was apparently not accepted by the legislature on this point. The general approach though, one which recognises a data controller's responsibility to protect

---

[23] *Aadhaar-5 Judge* (2019) 1 SCC 1.

[24] It is necessary to distinguish between 'fair' processing, which might be required by a respect for privacy, and 'fair' interference with privacy. Although one might expect a least a degree of consonance between tests of fairness in different parts of the same legal regime our interest is especially in the former.

[25] Lothar Determann and Chetan Gupta, 'India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018' (2019) 37(3) *Berkeley Journal of International Law* 481.

[26] We do not explore here the circumstances in which such uses might be considered a proportionate and legitimate curtailment of the right to privacy.

[27] The Aadhaar and Other Laws (Amendment) Act 2019. For commentary: see 'Lok Sabha Passes Aadhaar Amendment Bill', *The Economic Times* (online, 4 July 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/lok-sabha-passes-aadhaar-amendment-bill/articleshow/70078736.cms>.

individual interests through more than the safeguard of consent, was taken up in subsequent recommendations for regulatory reform.

B. Report of the Committee of Experts

Following the decision in *Puttaswamy,* a Committee of Experts — under the Chairmanship of Justice BN Srikrishna — submitted its report to the Ministry of Electronics and Information Technology on *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. The Committee clearly acknowledged the need for individual rights, including to privacy, to be balanced by collective interests.[28] Indeed, the Committee framed its recommendations on the twin bases that 'it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy', also served the 'common good'.[29] The Committee saw these as complementary objectives rather than being in conflict. This was because individual rights of autonomy were only meaningful in the context of a fair and equitable society. Thus

> [t]he growth of the digital economy, which is proceeding apace worldwide, must be equitable, rights reinforcing and empowering for the citizenry as a whole. In this, to see the individual as an atomised unit, standing apart from the collective, neither flows from our constitutional framework nor accurately grasps the true nature of rights litigation.[30]

The report recognised the role for consent in allowing data subjects to exercise autonomy.[31] It also acknowledged the concern that, particularly in an online environment, the operation of notice and consent are not strongly protective of individual rights.[32] However, it was not appropriate to abandon this mechanism altogether.[33] Consent-based mechanisms ensured respect for an individual's autonomy and also provided a clear basis for processing data.[34] Rather, there was a need for 'form and substance'[35] requirements to ensure consent in this context was meaningful; namely that consent be free, informed, specific, clear and capable of being withdrawn.[36]

---

[28] *Protecting Privacy, Empowering Indians* (n 10) 10.
[29] ibid 5.
[30] ibid 9.
[31] ibid 24.
[32] ibid 32.
[33] ibid 33.
[34] ibid 24.
[35] ibid 11.
[36] ibid 37.

Importantly, the Committee advocated strongly for an additional regulatory framework to ensure fairness in data processing which would provide a counter to the inevitable inequities of bargaining power between individuals and data principals.

Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated.[37]

The Committee recommended that the fair use of individual's data be achieved through the designation of a data fiduciary. Drawing on earlier scholarly work from the US, in particular the work of Balkin,[38] the committee explained that the fit of the fiduciary label arose from the expectations of the individual and the relationship of trust created between individuals and a data principal.[39] The Committee noted that such features were the 'hallmark' of a fiduciary relationship created in equity under common law regimes.[40] The duties of the data fiduciary should be to act consistently with that position of trust by complying with standards of fairness in the use of data.

In the digital economy, depending on the nature of data that is shared, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals.[41]

The Committee was clear that the 'fair and reasonable' requirement was more than a procedural duty but should have substantive content. These obligations should be premised on not processing data for ends that may not be in individuals' best interests or which go beyond their reasonable expectations.[42] Such obligations supplement consent as a safeguard for data privacy, but unlike rules for the way in which consent may be sought, go beyond consent as the determinant of the uses to which data can be put.

---

37 ibid 8.
38 Jack M Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49(4) *UC Davis Law Review* 1183.
39 ibid.
40 See, e.g., *Hospital Products Ltd v United States Surgical Corp Ltd* (1984) 156 CLR 41 ('*Hospital Products*').
41 *Protecting Privacy, Empowering Indians* (n 10) 8.
42 ibid 52.

C. The Personal Data Protection Bill 2019

The *Personal Data Protection Bill 2019* was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr Ravi Shankar Prasad, on December 11, 2019.[43] The Bill seeks to provide for protection of personal data of individuals and establishes a Data Protection Authority to that end. The Bill governs the processing of personal data by: (i) government, (ii) companies incorporated in India, and (iii) foreign companies dealing with personal data of individuals in India.[44]

Following the recommendations of the report of the Committee, the Bill establishes a central role for the consent of the 'data principal'; which is similar to the concept of the 'data subject' in the *GDPR*. Under section 11, personal data 'shall not be processed, except on the consent given by the data principal at the commencement of its processing'. However, sections 12, 13 and 14 provide other legal bases for processing. These include, under section 12, public functions authorised by law, and to respond to medical emergency or threat to public health. Section 13 provides for processing necessary in an employment context. Section 14 permits processing without consent if necessary, for 'reasonable purposes' as may be specified by the Regulations, taking into account respective private and public interests, whether it is reasonable to expect consent to be obtained, and the reasonable expectations of the data principal in the context.

Where consent is the lawful basis for processing, section 11(2) of the Bill states the consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;

---

[43] On the scope of the bill see further: Deva Prasad M and Suchithra Menon C, 'The Personal Data Protection Bill, 2018: India's Regulatory Journey Towards a Comprehensive Data Protection Law' (2020) 28(1) International Journal of Law and Information Technology 1; Determann and Gupta (n 25); Ashit Kumar Srivastava, 'Data Protection Law in India: The Search for Goldilocks Effect' (2019) 5(3) European Data Protection Law Review 408.

[44] For suggested improvements to strengthen privacy protection see Graham Greenleaf AM, 'India's Personal Data Protection Bill, 2019 Needs Closer Adherence to Global Standards' (Submission to Joint Committee, Parliament of India, 12 February 2020).

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such.[45]

This approach follows the recommendation of the Committee that the statutory requirements for valid consent should be a 'significant step towards ensuring the consent is informed and meaningful'.[46] The burden of proof that consent has been given is on the party who will be in control of the data, termed the 'data fiduciary',[47] but all legal consequences of a valid withdrawal of consent must be borne by the data principal.[48] It is not permissible to make provision of any good or service, performance of any contract, of enjoyment of any right or claim, conditional upon consent to the processing of personal data except where necessary for that purpose.[49]

In addition to establishing a higher threshold for a valid consent, again following the recommendations of the Committee, the Bill proposes a considerable role for the 'data fiduciary'. A data fiduciary is 'any person … who alone or in conjunction with others determines the purpose and means of processing of personal data.[50] Substantially the same definition is used for a 'data controller' under the *GDPR*.[51] The data fiduciary under the Bill is also under a responsibility to process personal data 'in a fair and reasonable manner and ensure the privacy of the data principal'.[52] The data fiduciary is also under an obligation to ensure that data is processed

for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.[53]

---

[45] Additional conditions attach to consent to the processing of sensitive personal data: see Personal Data Protection Bill 2019 (India) s 11(3).

[46] *Protecting Privacy, Empowering Indians* (n 10) 38–46; Annexure B; 185.

[47] Personal Data Protection Bill 2019 (India) s 11(5).

[48] ibid s 11(6).

[49] ibid s 11(4).

[50] ibid s 3. There is a further category of 'significant data fiduciary'. The Personal Data Protection Bill 2019 (India) s 26 establishes the conditions under which a data fiduciary may be defined as a significant data fiduciary, and thus subject to additional responsibilities.

[51] *GDPR* (n 14) art 4(7): 'controller' means 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

[52] Personal Data Protection Bill 2019 (India) s 5(a).

[53] ibid s 5(b).

i. Consent and Data Fiduciaries under the Indian Bill

As has been seen, one of the distinctive features of the Indian *Personal Data Protection Bill 2019* is its reliance on the concept of a data fiduciary. The use of the term 'fiduciary' to describe the obligations of the data controller is deliberate in order to invoke the equitable concept of a fiduciary. The classic description of a fiduciary in equity is a person who undertakes to act 'for or on behalf of or in the interests of another'.[54] Examples include doctors, lawyers and accountants. In adopting this approach, the Committee was influenced by the work of Professor Jack M Balkin.[55] Balkin observed that individuals are also dependent on, and vulnerable to the actions of, digital platforms such as Facebook, Amazon, Twitter and Uber. Because they hold special power to affect the well-being of others, Balkin argued that these digital platforms, and any business that collect, analyse, sell, use, and distribute data, should 'have special duties to act in ways that do not harm the interests' of the data principal.[56] Balkin accordingly proposed the concept of an information fiduciary applying to business and people in a digital age who 'collect, analyse, use, sell, and distribute personal information'.[57] Balkin's aim in developing this approach was to broaden the debate around protecting privacy from focusing on the kinds of data being held by an entity to the kinds of relationships between data subjects and data controllers that might justify regulation.[58] Balkin argued that if entities hold themselves out as trustworthy in holding personal information, they should be held to these assertions.[59] The framework has been criticised by other scholars, prominently by Khan and Pozen.[60] They argue that the technique of using fiduciary law to address concerns about how data is handled by companies fails to address the systematic issues of 'structural power' around digital platforms and the need for 'more robust public regulation'.[61] Khan and Pozen also question the fit between the fiduciary concept, even in the modified form

---

[54] *Hospital Products* (n 40) 96–7 (Mason J). In US jurisprudence, see *Kurtz v Solomon* 656 NE 2d 184, 190 (III App Ct, 1995); Tamar Frankel, *Fiduciary Law* (Oxford University Press, 2011) 42–5; Deborah A DeMott, 'Beyond Metaphor: An Analysis of Fiduciary Obligation' [1988] (5) Duke Law Journal 879, 882.

[55] Balkin (n 38). See also Lina M Khan and David E Pozen, 'A Skeptical View of Information Fiduciaries' (2019) 133(2) *Harvard Law Review* 497.

[56] Balkin (n 38) 1186.

[57] ibid.

[58] ibid 1187.

[59] ibid 1224.

[60] Khan and Pozen (n 55).

[61] ibid 502.

proposed by Balkin, and the business models of digital platforms who would be the prime exemplars of the new data fiduciary designation,[62]

In the Indian *Personal Data Protection Bill 2019*, the concept of the data fiduciary has been extended more generally to address fundamental concerns about the ability of data subjects to adequately protect their own interests purely through mechanisms based on consent and contract. The Committee of Experts, whose recommendations shaped the Bill, explained that the use of the term fiduciary in the data protection context was a recognition not only that the relationship between contracting parties may be unequal, but of 'one party's dependence on another for performance of a service or achievement of an objective'.[63] This imbalance in bargaining power and consequent dependence on the decisions of the data controller characterises many online transactions where a consumer may not have any alternative other than to agree to provided terms and conditions, if they wish to receive a service or achieve another objective.

In equity fiduciaries are subject to a rigorous set of protective obligations. The Committee of Experts observed that fiduciaries must uphold 'trust and loyalty placed in them by the data principal'.[64] This takes the form of a duty to act 'in the best interest of the principal'.[65] In general fiduciary relationships this requires the fiduciary to avoid conflicts of interest [66]and taking unauthorised profits from their position as fiduciary.[67] It does not appear that the data fiduciary under the Indian *Personal Data Protection Bill 2019* is intended to hold the same set of stringent expectations around loyalty, and indeed Balkin's model of an information fiduciary a more limited set of expectations than might apply to traditional kinds of fiduciary.[68] As Khan and Pozen have pointed out, avoiding conflicts would be practically impossible for many key players in the digital economy.[69] The committee of experts described the responsibilities of the data fiduciary as requiring it not to

---

[62] ibid 507. See also 511 discussing the tension between fiduciary duties of loyalty and targeted advertising.

[63] *Protecting Privacy, Empowering Indians* (n 10) 51.

[64] ibid.

[65] ibid. See, eg, *Breen v Williams* (1996) 186 CLR 71, 135 (Gummow J); *Pilmer v Duke Group Ltd* (2001) 207 CLR 165, 199 [78] (McHugh, Gummow, Hayne and Callinan JJ) ('*Pilmer*'). See also Deborah A DeMott, 'Breach of Fiduciary Duty: On Justifiable Expectations of Loyalty and Their Consequences (2006) 48(4) *Arizona Law Review* 925.

[66] *Pilmer* (n 65) 199 [78] (McHugh, Gummow, Hayne and Callinan JJ); *Hospital Products* (n 40) 103 (Mason J); *Boardman v Phipps* [1967] 2 AC 46: [1966] 3 WLR 1009, 127 (Lord Upjohn).

[67] For the interaction between these two 'overlapping but distinct' themes, see *Chan v Zacharia* (1984) 154 CLR 178, 198–9 (Deane J).

[68] Balkin (n 38) 1225.

[69] Khan and Pozen (n 55) 504.

process data in a way that goes beyond the reasonable expectations of the data principle or in a way that was not in the data principal's best interests.[70] The *Personal Data Protection Bill 2019* sets out a more narrowly focused set of duties, focused on protecting the privacy interests of the data subject, rather than avoiding conflicts of interest. In particular, as noted above, the data fiduciary's obligations are to process personal data 'in a fair and reasonable manner and ensure the privacy of the data principal'.[71] The scope of protection is determined by reference to the purposes that the data principal would reasonably expect, having regard to 'the purpose, context and circumstances of the collection'.[72]

Whether this formulation of the data fiduciaries' duties leaves any real resonance with the general law concept of a fiduciary is not, for our purposes, a necessary debate. It may be that different language would be preferable to avoid confusion around the equitable and statutory concepts.[73] We also do not here engage with the broader issue of whether the structural imbalances in power that characterise a modern information economy should be addressed in more direct ways, including an entire restructuring of the market. Khan and Pozen are certainly concerned that Balkin's concept of a data fiduciary may prove an unhelpful distraction from the broader reforms required.[74] We wish to focus solely on the decision in the legislature to impose subjective restrictions on data processing that apply regardless of the existence of consent, or for that matter, contract, of the data subject. In this context, we observe that the label 'data fiduciary' seems to be to have an iterative function in emphasising that the data controllers' duties go beyond acting in its own commercial self-interest. A move to make clear that protecting the reasonable expectations of the data subject to data privacy is the responsibility of the data controller/data fiduciary. Placing the defined positive obligations on the entity that determines the purpose and means of processing of personal data extends responsibility beyond technical compliance with a duty to ensure a legal basis for processing.

> Placing such an obligation is recognition of the fact that given the unequal nature of the relationship and its inherent opacity, what is legal may not ipso facto be fair or reasonable.[75]

---

[70] *Protecting Privacy, Empowering Indians* (n 10) 52.
[71] Personal Data Protection Bill 2019 (India) s 5(a).
[72] ibid s 5(b).
[73] Cf Jeannie Marie Paterson and Elise Bant, 'Mortgage Broking, Regulatory Failure and Statutory Design' (2020) 31(1) Journal of Banking and Finance Law and Practice 7.
[74] Khan and Pozen (n 55) 502.
[75] *Protecting Privacy, Empowering Indians* (n 10) 52.

The effect of this strategy is that the fiduciary has obligations to assess the consequences of data use and cannot rely on consent as permission for a specified use. A consumer's consent to processing is not sufficient guarantee that the processing is either in their best interests or fair and reasonable. Consumers cannot be presumed to be capable of protecting their own interests when it comes to privacy and the common law concept of 'reasonable expectations' remains critical in defining the acceptable limits of data processing. As noted by the Committee:

> Further it is testament to the fact that consent which may be valid for creating legal relationships may not be sufficient to fully disclaim liability.[76]

The Committee does not suggest that the standard of fair and reasonable will unpack in the same way in all circumstances:

> Needless to say, the extent of the obligations of a data processor may differ, depending on the exact nature of processing in question and the requisite duty of care may be duly reflected in the contract between the data fiduciary and itself.[77]

They saw the flexibility within the standard, and the discretion it afforded the regulator and courts to do justice in the instant case, to be a strength:

> This is precisely why laying down such a general principle of fair and reasonable processing will allow it to be developed by the DPA and courts of law, taking into account technological developments over time and differential obligations of different entities.[78]

There is little doubt that this move leaves many questions unanswered. Should the obligations of online sellers be the same as those of social media platforms or online banking service providers?[79] What happens if the data fiduciary is a public rather than a private body? How do these circumstances affect what constitute 'reasonable expectations'? These are important questions to be resolved. Without answering them ourselves, we can note the value of prospective regulatory guidance. Our point is only that the opportunity to promote a contextual understanding of what constitutes a valid consent in different circumstances is valuable. This is something that seems

---

[76] ibid.
[77] ibid.
[78] ibid.
[79] We note that the Bill itself proposes some answers to such questions by elevating the obligations of a 'significant data fiduciary' and including 'social media intermediary' within the latter class: seen n 58. This does not, however, preclude further debate on how obligations should be distributed across different kinds of data controller.

to be becoming less, rather than more, nuanced under European data protection legislation.

III. A European Perspective

We can see within European data protection law similar signs of ambivalence with regards to the function of consent as we have previously noted. It is a central data protection safeguard. But it remains unresolved whether informational self-determination is valued for its own sake or as a means to prevent misuse of personal data: with 'misuse' defined relative to a conception of reasonable expectation that is at least partially independent of the data subject.[80] The proper function of consent in European law is further complicated by the fact that European data protection law has moved to disconnect a right to data protection from the right to privacy[81]. This also opens many questions we do not seek here to pursue. We wish only to note that — irrespective of any underlying normative or conceptual coherence — this move has been accompanied by a strengthening of the requirements for a valid consent beyond that anticipated by the Indian *Personal Data Protection Bill 2019* and a trend toward recommending reliance upon legal basis *other than* consent to legitimise processing. We offer UK data protection law as an example of a regime that has raised the bar for individual consent, recommended that alternatives be relied upon when available, and not applied the test of *unfair* processing in a way that demonstrates it to have the substantive content proposed by the Expert Committee in India. The result, we suggest, is a missed opportunity to progress either a welfarist or individualist agenda: individuals are not effectively empowered in practice, nor are agreements regulated to protect the best interests of either individuals or society more generally.

---

[80] We do not have the space here to fully unpack a conception of 'reasonable expectation' but we note that the classic US formulation of 'reasonable expectation,' dating back to *Charles Katz v United States* 1967 SCC OnLine US SC 248: 19 L Ed 2d 576 : 389 US 347 (1967), has both a subjective and an objective element. We would connect an understanding of 'fair processing' to the objective element. One of us has written more on the concept of a reasonable expectation in the context of the English law of confidence. Mark J Taylor and James Wilson, 'Reasonable Expectations of Privacy and Disclosure of Health Data' (2019) 27(3) *Medical Law Review* 432. The systematic consideration of the conceptual relationship between the term as used in different contexts, and the notion of 'fair' in data protection law, must wait for future research.

[81] See further Bart van der Sloot 'Legal Fundamentalism: Is Data Protection Really a Fundamental Right?' in Ronald Leenes et al (eds), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017) 3 exploring the question of what it means for EU law to have separated data protection from the right to privacy and instead to have elevated data protection to the level of a fundamental right.

The EU *General Data Protection Regulation* ('*GDPR*') (2016/679) repealed and replaced the *European Data Protection Directive* (95/46/EU). It came into force on 25 May 2018 and was intended to not only update European data protection law but also, as a regulation (rather than a directive), to achieve higher levels of harmonisation across Europe. In the UK, any processing[82] of personal data carried out in the context of an establishment of a controller or processor in the UK,[83] must comply with data protection legislation,[84] including the *Data Protection Act 2018* and the *GDPR* as applied in the UK context.

The term 'personal data' is defined very broadly by data protection legislation to include *any* information relating to an identified or identifiable person.[85] Those subject to the requirements of data protection legislation must process personal data in compliance with a set of data protection principles which relate to 'lawfulness, fairness, and transparency', 'purpose limitation', 'data minimisation', 'accuracy', 'storage limitation', 'integrity and confidentiality', and 'accountability'. The lawfulness of processing is determined, in part, by Article 6 of the *GDPR*.

It is necessary (but not sufficient) for lawful processing to meet one of the conditions set out in Article 6(1) of the *GDPR*. The conditions most likely to be appropriate to processing for research purposes are (i) processing is with the data subject's consent (Article 6(1)(a)), (ii) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)), or (iii) processing is necessary for the purposes of a data controller's legitimate interests (Article 6(1)(f)). Only one condition needs to be satisfied. A data subject's consent is not required if an alternative ground is available. Controllers should select the most appropriate ground available for the processing intended.

---

[82] Broadly defined by *GDPR* (n 14) art 4(2) to include any operation or set of operations performed on personal data or on sets of personal data whether or not by automated means.

[83] Data Protection Act 2018 (UK) s 207(2). In fact, the territorial application of the 2018 extends beyond this. This is a point we pick up later as it has some significance for researchers in member states targeting research participants in the UK in case of Brexit.

[84] ibid s 3(9) provides a definition of data protection legislation. To be amended, in case of Brexit by Sch 21, Pt 2, Para 2(1) of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[85] *GDPR* (n 14) art 4(1) defines 'personal data' as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Special categories of data qualify for additional protections under data protection law, through Article 9 of the *GDPR*. Processing of special category data is prohibited unless one of a number of exceptions apply. The first alternative exception under Article 9 is that 'the data subject has given explicit consent to the processing' (Article 9(2)(a)).

'Consent' is thus both an available lawful basis for processing (under Article 6) *and* 'explicit consent'(an available exception to the prohibition on processing special category data (under Article 9)). Consent is defined by the *GDPR* to mean

> any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.[86]

The *GDPR* is understood to have raised the threshold for a valid consent under EU data protection law and represents

> an important reframing of the consent standard in terms of greater specificity of requirements and more stringent protection of participants. The consent framework is expanded upon in several of its Recitals (particularly 32, 33, 40, 42, 43, 157 and 171), as well as in Articles 7 (on the conditions for consent), 8 (on a child's consent relating to information society services) and 17 (on the right to erasure).[87]

This has led to a move away from a reliance upon consent.[88] The data protection authority in the UK, the Information Commissioner's Office ('ICO'), advises that:

> The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.[89]

---

[86] *GDPR* (n 14) art 4(11).

[87] Megan Prictor et al, 'Consent for Data Processing Under the General Data Protection Regulation: Could 'Dynamic Consent' be a Useful Tool for Researchers?' (2019) 3(1) *Journal of Data Protection and Privacy* 93, 96.

[88] Olly Jackson, 'Businesses Retreating from Consent Under GDPR', *International Financial Law Review* (online, 3 April 2018) <https://www.iflr.com/Article/3798060/Businesses-retreating-from-consent-under-GDPR.html>.

[89] Information Commissioner's Office (Guide), 'Guide to the GDPR: Lawful Basis for Processing: Consent' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/>.

The *GDPR* itself discourages reliance upon consent where the controller is a public body or where there might otherwise be a clear imbalance of power between the parties:

> In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.[90]

This threshold for a 'free' consent thus appears higher than that under the Indian *Personal Data Protection Bill 2019*, where it is sufficient to comply with the standard specified under section 14 of the Indian *Contract Act 1872*: namely that it is not caused by coercion, undue influence, fraud, misrepresentation or mistake.[91] It is questionable, however, whether raising the bar in this way — and discouraging consent in any case of clear imbalance of power, irrespective of whether that imbalance is abused — is empowering if it encourages organisations to rely upon alternative legal bases.

If consent is not the legal basis, then there is some protection for individual or collective interests built into the alternatives but not necessarily in consistent measure. If processing is by a public body, then processing shall be lawful to the extent it is 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' (Article 6(e)). This clearly restricts the freedom of public bodies to act in pursuit of a self-interested agenda without adequate account taken of the public interest evidenced either in the specific task or in the original allocation of official authority. Private bodies may rely upon 'legitimate interests' (Article 6(1)(f)) or on the requirement that processing is necessary for the performance of a contract to which the data subject is party (Article 6(1)(b)). If reliant on the former, then they must consider whether their interests in processing are overridden by the individual's interests or fundamental rights and freedoms. A controller can rely upon processing being necessary

> for the purposes of the legitimate interests pursued by the controller or by a third party, *except where such interests are overridden by*

---

[90] *GDPR* (n 14) Recital 43.

[91] 'Consent is said to be free when it is not caused by (1) coercion, as defined in Section 15, or (2) undue influence, as defined in Section 16, or (3) fraud, as defined in section 17, or (4) misrepresentation, as defined in Section 18, or (5) mistake, subject to the provisions of Sections 20, 21 and 22. Consent is said to be so caused when it would not have been given but for the existence of such coercion, undue influence, fraud, misrepresentation or mistake'.

> *the interests or fundamental rights and freedoms of the data subject* which require protection of personal data, in particular where the data subject is a child.[92]

While this puts no obligation on a data controller to act in the interests of a data subject, nor consider collective concerns, it does constrain the ability of the data controller to pursue their own interests in a way that disproportionately impacts upon an individual. If reliant on the fact that processing is necessary for the performance of a contact to which the data subject is party, then the interests of an individual are narrowly protected by a requirement that the processing be necessary given the contractual purpose. The Article 29 Working Party opined that this legal basis applies to prevent unilateral imposition on a data subject through a contract:

> For example, Article 7(b) is not a suitable legal ground for building a profile of the user's tastes and lifestyle choices based on his click-stream on a website and the items purchased. This is because the data controller has not been contracted to carry out profiling, but rather to deliver particular goods and services, for example. Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them 'necessary' for the performance of the contract.[93]

Of course, this does not preclude a data subject from contracting for services, such as profiling, in circumstances where others might question whether the service is in the individual's best interests.[94] Where processing *is* on the basis of an individual's consent, then even these uneven levels of protection for individual and collective interests do not apply. When consent is the lawful basis, then the expectation is that the data subject is best placed to protect his or her best interests. As the Article 29 Working Party put it:

> In the first case, under Article 7(a), it is the data subjects themselves who authorise the processing of their personal data. It is up to them to decide whether to allow their data to be processed …. As the processing of the user's data is ultimately at his/her discretion, the emphasis is on the validity and the scope of the data subject's consent. In other words, the first ground, Article 7(a), focuses on the self-determination of the data subject as a ground for legitimacy. All other grounds, in contrast, allow processing — subject to safeguards and measures

---

92 *GDPR* (n 14) art 6(1)(f) (emphasis added).

93 European Commission, 'Opinion 06/2014 on the Notion of legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC', 844/14/EN WP 217, 17.

94 The interests of the data subject are, however, not here to be protected via data protection law, but rather through consumer protection measures in commercial and contract law.

> — in situations where, irrespective of consent, it is appropriate and necessary to process the data within a certain context in pursuit of a specific legitimate interest.

There are other specific examples where it is left to an individual, through the consent mechanism, to protect their own interests. We briefly mention just two. The first relates to automated processing, and here there is a clear intent to ensure some level of protection does persist. The second relates to transfer of data outside of the European Union and the protective regime of the *GDPR*. Here, however, it is much clearer that a data subject is entitled to agree to an arrangement that leaves them with materially less protection without proportionate benefit.

First, the *GDPR* states that individuals should have the right not to be subject to a decision based solely on automated processing.[95] However, decision-making based on such processing should be allowed 'when the data subject has given his or her explicit consent'.[96] In this case, the data controller is required to suitably safeguard the data subjects' rights, freedoms and legitimate interests and the data subject has 'at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision'.[97] There is thus a continued requirement to safeguard the individual's interests, but the level of protection is not the same. There is a level of risk that a data subject is entitled to take on by waiving the right not to be subject to decisions based solely on automated processing, and there seems no requirement that it be in his or her best interests to do so.

Chapter V of the *GDPR* (especially Articles 44 to 48) establishes the rules for transfer to a 'third country' and makes clear the underlying principle that such transfer ought not to undermine the level of protection guaranteed by the Regulation. However, Article 49 does allow for derogations for specific situations. One of these is that:

> The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject.

If a data subject *has* been informed of the risks, and he or she provides a valid consent, then he or she is entitled to assume the risks of the transfer. This is the case even though a data controller is likely to have involved a third country for their own reasons and to their own advantage. For example, a

---

[95] *GDPR* (n 16) art 22(1).
[96] *GDPR* (n 16) recital 71; art 22(2)(c).
[97] ibid art 22(3).

data subject might be asked to accept risks which are associated with cheaper processing operations for the data controller. There is no requirement that the transfer to a third country be in the best interests of the data subject. There is only the underlying assumption that if the processing operation overall was not in his or her interests, they would not agree to it.

A. Fair Processing

Of course, any processing operation must not only be 'lawful' but must also satisfy other data protection requirements. Additional requirements may remedy any lack of protection associated with processing on the basis of a data subject's consent. Perhaps the most pertinent is that processing must be 'fair', as well as lawful.

Article 8 of the *Charter of Fundamental Rights of the European Union* requires that personal data must be processed 'fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'.[98] The first data protection principle set out by the *GDPR* is that data shall be 'processed lawfully, *fairly* and in a transparent manner' (emphasis added).[99] When identifying the appropriate legal basis, data controllers must 'take into account the impact on data subjects' rights … in order to respect the principle of fairness'.[100]

In online guidance, the UK data protection regulator, the Information Commissioner's Office ('ICO') answers the question 'What is fairness?' in the following way:

> In general, fairness means that you should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them. You need to stop and think not just about how you can use personal data, but also about whether you should.
>
> […]
>
> In order to assess whether or not you are processing personal data fairly, you must consider more generally how it affects the interests of the people concerned – as a group and individually. If you have obtained and used the information fairly in relation to most of the

[98] Charter of the Fundamental Rights of the European Union [2012] OJ C 326/391, art 8(2).
[99] *GDPR* (n 16) art 5(1)(a).
[100] European Data Protection Board, 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects' (Guide, 16 October 2019) 4.

> people it relates to but unfairly in relation to one individual, there will still be a breach of this principle.[101]

This guidance suggests that the requirement that data is processed fairly may operate to constrain adverse effects on people, both as individuals and as members of groups. Superficially, there appear many parallels with the requirement for fair and reasonable processing proposed in the Indian *Personal Data Protection Bill 2019*. However, there is no parallel notion of a data fiduciary and there is some indication that this requirement has functioned to protect an idea of 'fair' that is tied closely to a procedural rather than substantive conception of fairness: requiring transparency and action consistent with declared intention, avoiding duplicity or misleading practice.[102] This does not, however, include the requirement that fair processing necessarily must also be in the interests of the data subject.

The Hellenic Data Protection Authority, in response to a complaint against PricewaterhouseCoopers ('PwC'), found that PwC had failed to process personal data relating to employees fairly. PwC required employees to provide consent to the processing of their personal data. This was considered an inappropriate legal basis in the circumstances. The Authority concluded that PwC

> [p]rocessed the personal data of its employees in an unfair and non-transparent manner … given them the false impression that it was processing their data under the legal basis of consent … while in reality it was processing their data under a different legal basis about which the employees had never been informed.[103]

One of the concerns with the fact that employees had been misled as to the legal basis upon what data was being processed was that this created a false impression of the control they might exercise over that processing: 'the choice of each legal basis has a legal effect on the application of the rights of data subjects'. There was no suggestion that PwC could not process the personal data for the purposes they had been processing it or that employees

---

[101] Information Commissioner's Office (Guide), 'Guide to the GDPR: Principles: Lawfulness, Fairness and Transparency' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/>.

[102] Damian Clifford and Jef Ausloos have suggested that two key elements may be distilled from the fairness principle in European data protection law: fair balancing (proportionality and necessity) and procedural fairness. See Damian Clifford and Jef Ausloos 'Data Protection and the Role of Fairness' [2018] *Yearbook of European Law* 1.

[103] 'Price Waterhouse Coopers Business Solutions: Summary of Hellenic DPA's Decision' (Decision Summary No 26/2019, 2019) <https://edpb.europa.eu/sites/edpb/files/files/news/summary_of_decision_26_2019_en_2.pdf>.

must have more control than they did; the problem was that they had misled employees and sought to transfer compliance obligations to them by relying upon consent rather than a more appropriate legal basis.

The UK Data Protection Authority found that the processing by Royal Free NHS Foundation Trust ('Royal Free') did not fully comply with the requirements of the *Data Protection Act 1998*. Royal Free provided a third party, DeepMind, with approximately 1.6 million patient records under agreement for the purposes of carrying out clinical safety testing as part of the development of a new clinical detection, diagnosis and prevention application for the Trust in relation to Acute Kidney Injury. The Authority found that:

> The processing of patient records by DeepMind significantly differs from what data subjects might reasonably have expected to happen to their data when presenting at the Royal Free for treatment.[…] The mechanisms to inform those patients that their data would be used in the clinical safety testing of the Streams application were inadequate. In short, the evidence presented to date leads me to conclude that data subjects were not adequately informed that the processing was taking place and that as result, the processing was neither fair nor transparent.[104]

If the mechanisms to inform patients that data would be used in this way *had* been adequate, then the implication is that the processing would not have been unfair. No substantive judgement was made about the fairness of Royal Free patient data being processed by DeepMind. There was no substantive consideration given to whether the processing was in the interests of the patients whose data was transferred; only whether patients might reasonably expect it in the circumstances.

IV. Reflection and Recommendations: The Function and Limits of Consent

The Indian *Personal Data Protection Bill 2019* raises the threshold for valid consent, allows processing without consent in a limited range of circumstances, but places an obligation on data fiduciary to process 'fairly and reasonably' irrespective of consent to the processing. This is in recognition of the unequal bargaining positions of data principal and data controller. It is

[104] Information Commissioner's Office, 'DeepMind: Undertaking Cover Letter' (Notice of Investigation and Findings, 3 July 2017) <https://ico.org.uk/media/action-weve-taken/undertakings/2014353/undertaking-cover-letter-revised-04072017-to-first-person.pdf>.

intended to carry substantive content, and the use of the term 'data fiduciary' reinforces this position.

This approach may provide more significant protection than under European data protection law for which we have taken UK law as an example. This is even though a number of the provisions in the Indian *Personal Data Protection Bill 2019* appear analogues of those in European data protection law, and also despite the fact that the threshold requirements for consent may even be higher under UK law than under the Indian *Personal Data Protection Bill 2019*. In fact, raising the level of valid consent may be counterproductive.

The goal, if relying on consent to provide the legal basis for processing, presumably lies in the judgment that this mechanism will produce beneficial outcomes for individuals and for the market. In principle, individuals consent to processing only where they consider it to represent a fair bargain: consent itself is a sign of perceived mutual benefit. The stance taken in data protection regimes of imposing high threshold requirements for valid consent may be steps toward empowering consumers to strike bargains only when it is perceived to be in their best interests to do so. If it is a win-win scenario, then the consumer's interests may be sufficiently protected. A similar principle informs the law of contract and is expressed in the idea of 'freedom of contract'.

However, consent is a fragile means of protecting individual rights. As the Indian Expert Committee noted, one commonly expressed view is that consent in online contexts is 'broken'.[105] Consent in the context of online transactions or standard form contracts is not an adequate, or even accurate, indicator of the preferences of the individuals that give it, nor guaranteed to lead to welfare enhancing outcomes. Statutory mechanisms may seek to protect individuals against so called 'forced' consent by requirements — such as found in both the Indian *Personal Data Protection Bill* and the *GDPR* — for consent to be free, informed, specific, clear and capable of being withdrawn. These protections will be buttressed by prohibitions on misleading conduct and coercion provided under contract law[106] and consumer protection legislation.[107] However, they do little to get to the heart of the limitations on consent as an autonomy enhancing measure, which lies in the bounded rationality of human decisionmakers.

---

[105] *Protecting Privacy, Empowering Indians* (n 10) 32.
[106] See, eg, the Indian Contract Act 1872, s 15 (coercion) and s 18 (misrepresentation).
[107] See further the Consumer Protection Act 2019 (India).

Studies suggest that there are cognitive limitations on the ability of individuals to assess the risk allocations embedded in particular terms.[108] Individuals tend to estimate the probability of risk by reference to their experience or knowledge of the risk. Thus, individuals 'judg[e] risk to be high when the type of harm is familiar or easily imagined and low when it is not'.[109] They tend to be overly optimistic about their abilities to avoid risk. Moreover, hyperbolic discounting means that 'individuals systematically overvalue immediate benefits and costs and undervalue delayed benefits and costs'.[110] For these kinds of reasons, consumer protection law now commonly contains principles that can also impose substantive protections about the kinds of things that can be consented to including through scrutiny of unfair contract terms.[111] The proposed Indian *Personal Data Protection Bill 2019 i*s notable in that substantive protections are, as we have already noted, included as a counter balance to the notion of consent. The requirement for consent, or available exception, is supplemented by a requirement that personal data only be processed in a way that is 'fair and reasonable'. This obligation is given to the data controller or fiduciary. In so doing the Bill emphasises, in our view, that the requirement of fair and reasonable processing is not a mere procedural requirement but a substantive obligation. It requires, in our view, the data fiduciary to have regard to the interests of the data subject and at least ensure their interests are not undermined in a manner that is disproportionate to the goals to be achieved. It may also allow the data fiduciary to consider the interests of the data principal by reference to social values and expectations. Just how this balance is struck depends on the view taken of the interests that can justifiably be set against the privacy rights of the individual, leading to questions about the appropriate priorities as between public/private, present/future and individual/group interests should be set. Our point in this paper is that such limits should be seen as central part of a functioning data protection system.

---

[108] See, eg, Russel Korobkin, 'Bounded Rationality, Standard Form Contracts, and Unconscionability' (2003) 70(4) University of Chicago Law Review 1203; Robert A Hillman and Jeffrey J Rachlinski, 'Standard Form Contracting in the Electronic Age' (2002) 77(2) New York University Law Review 429; Melvin Aron Eisenberg, 'The Limits of Cognition and the Limits of Contract' (1995) 47(2) Stanford Law Review 211; Genevieve Helleringer and Anne-Lise Sibony, 'European Consumer Protection Through the Behavioral Lense' (2017) 23(3) Columbia Journal of European Law 607.

[109] Korobkin (n 108) 1233.

[110] Jason J Kilborn, 'Behavioral Economics, Overindebtedness and Comparative Consumer Bankruptcy: Searching for Causes and Evaluating Solutions' (2005) 22(1) *Emory Bankruptcy Developments Journal* 13, 21. See also Jon D Hanson and Douglas A Kysar, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' (1999) 74(3) *New York University Law Review* 630, 678–680; Cass R Sunstein, 'Behavioral Analysis of Law' (1997) 64(4) *University of Chicago Law Review* 1175, 1193–4.

[111] Consumer Protection Act 2019 (India).

V. Conclusion

The proposed Indian *Personal Data Protection Bill 2019* takes steps to ensure that consent to personal data processing in India is informed and meaningful. It does not, however, stop there. The Bill seeks also to recognise more broadly the conditions necessary for trust in a modern information economy; placing responsibilities on organisations to not abuse the inevitable inequities in relative bargaining positions. The Srikrishna Committee, commenting on the proposed Bill, recognised the importance of consent as a safeguard but emphasised also that a privacy and data protection framework must serve 'the common good'.

We have not sought to answer the perennial question, 'What constitutes the common good?'. We have, however, suggested that whether one's sympathies lie toward a 'market individualist' or 'consumer welfarist' ideal of society, there are merits in a substantive test for 'fair processing'. Whether the intent is only to safeguard the ability of the individual to take decisions, or to protect interests and values beyond individual autonomy and information self-determination, it is necessary to go beyond consent. The role of a data fiduciary, as currently conceived under the Indian *Personal Data Protection Bill 2019*, gives more substance to the idea of what it means for a data controller to act fairly in relation to a data subject than has hitherto been applied by data protection authorities in Europe. It goes beyond the idea that organisations should be transparent and avoid misleading or deceptive practices. It places a responsibility upon the organisation to act in a way that is both 'fair and reasonable'.

Interpretation and application of 'fair and reasonable' under Indian law will be shaped by the case of *Justice KS Puttaswamy* v. *Union of India* (2017). In this case the Indian Supreme Court established the right to privacy is a fundamental right under Article 21 of the Indian Constitution. The Supreme Court indicated data protection and informational privacy is encompassed by the right to privacy. One can expect there to be normative implications associated with this pedigree; divorcing the right to data protection from a right to privacy in European data protection law may lead to different expectations being considered to be reasonable. The opacity of key concepts and their interconnectedness, concepts such as autonomy, liberty and human dignity, leaves a lot of scope for judicial interpretation of a 'reasonable expectation' in both jurisdictions. Different explanations for right to privacy, and its relationship with data protection, have different implications for scope and content of a right to fair processing, and the relationship to, and function of, individual consent as a safeguard. While the proper function of consent

may remain obscure while the philosophical underpinnings are moot, there is little doubt that it is no longer sufficient a device to progress even an individualist agenda.

A thin notion of consent that is not buttressed by other kinds of protection, both procedural and substantive, does not guarantee either autonomy or privacy. This is not to undermine the significance of consent. On the contrary, our argument is that if properly supported by a substantive test of fairness, there is less need to operate with the high threshold for valid consent that may discourage reliance upon consent as the legal basis for processing. The proper response to a recognition that consent is currently 'broken' in many online contexts is neither to abandon it, nor to try to fix it by ever higher thresholds for valid consent. The proper response is to complement it with other safeguards that protect the underlying values and interests at stake. Whether these are articulated in ways that display individualist or welfarist tendencies, there is an important role to be played by a test for 'fair and reasonable' processing: guaranteeing that data will not be processed for ends that may be harmful to data principals or which go beyond their reasonable expectations.

Although the judgment in *Puttaswamy* shows the ambivalence we have noted, the point is that whichever conception of privacy is preferred, and whatever that means for the role of consent within privacy and data protection law, there has been a recognition in India that it is necessary to move beyond consent to a more substantive test of 'fair and reasonable'. Consent and substantive fairness protections should not be seen as diametrically opposed requirements, one presenting respect for individual's right themselves to make the decisions that affect their lives and the other a paternalistic intrusion by the state to promote collectivist goals. Rather, once it is recognised that there are limits to the work that can be done by consent in protecting individuals' reasonable expectations of privacy, then substantive safeguards may be seen as both autonomy enhancing, by allowing individuals scope to live their lives to the fullest without being responsible for endless decisions affecting their future selves, as well as promoting more collectivist goals. Indeed, those goals of substantive fairness may be seen as an expression of community expectations that the state will indeed take actions to protect the interests of its citizens in order to preserve fundamental values that benefit them individually and as members of a community, both presently and into the future.[112]

[112] Cartwright (n 1) 37. See also Mindy Chen-Wishart, 'Controlling Unfair Terms: Protecting the Institution of Contract' in Louise Gullifer and Stefan Vogenauer (eds), *English and*

VI. Acknowledgements

We would like to sincerely thank Radhika Sarda and Devansh Kaushik, LLB (Hons) candidates at the National Law School of India University for their assistance with the preliminary research for this article and for the very helpful and constructive comments of the anonymous reviewer. We would also like to sincerely thank Yi Tung, JD Candidate at the University of Melbourne for assistance with referencing, formatting and copy-editing the final work. We are very grateful for the valuable help provided. This would not have been written without you.

European Perspectives on Contract and Commercial Law: Essays in Honour of Hugh Beale (Hart Publishing, 2017) 105.