PRESERVING CONSENT WITHIN DATA PROTECTION IN THE AGE OF BIG DATA

Kritika Bhardwaj*

The principles of notice and consent have come to form the bedrock of most modern data protection statutes. With the rise of big data technologies, which are inherently based on the collection and processing of a large amount of personal information, the effectiveness of consent as the basis for data processing is increasingly being called into question. This paper attempts to refocus the debate on consent in the context of autonomy and choice, which is integral to the right to privacy. It argues that in light of the Indian Supreme Court's categorical finding to this effect, the principle of consent must not only be retained but also further strengthened under India's imminent data protection statute.

In this light, this paper critically examines a few proposed alternatives to the notice and consent paradigm. However, being alive to the practical constraints in implementing the consent principle successfully, this paper advocates for additional legal and regulatory safeguards in order to reinforce and strengthen the principle, instead of replacing it altogether.

I. Introduction

The right to privacy has famously eluded a concrete definition.[1] Over time, concepts such as secrecy, confidentiality, the right to be let alone, surveillance and freedom from search and seizure have been associated with it, depending on the context.[2] However, there is a surprising coherence in ascribing a definite, beneficial value to the right,[3] as most recently affirmed by the Supreme Court of India, where it identified the right to privacy as being essential for liberty, autonomy and the ability to live with dignity.[4]

* Kritika Bhardwaj is an advocate practising in Delhi.

1 Ruth Gavison, 'Privacy and The Limits Of Law' (1980) 89 The Yale Law Journal 421.

2 Daniel J Solove, 'Conceptualizing Privacy' (2002) 90 California Law Review 1087.

3 Tom Gerety, 'Redefining Privacy' (1977) 12 Harvard Civil Rights – Civil Liberties Law Review 233; Alan F Westin, *Privacy and Freedom* (first published 1967, IG Publishing 2015); Edward J Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 New York University Law Review 962.

4 *K Puttaswamy v Union of India* (2017) 10 SCC 1 (Puttaswamy Case).

The recognition of autonomy as an inherent facet of the right to privacy is of great significance in the context of data protection. Data protection legislations, which seek to regulate the flow of personal information from individuals to public and private entities, have largely come to rely on the principle of consent to facilitate autonomy and individual choice.[5] In practice, however, consent has proven to be ineffective in adequately shielding individuals from privacy violations.[6] Further, the emergence of big data has only raised more questions about the appropriateness of consent in safeguarding privacy.

This paper looks at the recent debates surrounding the obsolescence of the consent principle through the lens of autonomy, and emphasises on its importance in understanding and securing privacy. It explores the constitutional foundations of consent and advocates for its inclusion within the data protection framework, albeit with added technological or regulatory safeguards.

The paper is divided into five parts. The second part explains the principle of consent under data protection law in greater detail. It also locates the principle within Indian constitutional jurisprudence on the right to privacy and argues for its incorporation into India's imminent data protection law on this basis. The third part discusses the causes and consequences of an imperfect consent regime and highlights a few proposed alternatives to the prevailing model. The fourth part critiques these alternatives and advocates the incorporation of consent within a principle-based data protection framework based on, and in furtherance of, the fundamental right to privacy.

II. Locating Autonomy in Data Protection Law – Notice and Consent

Data protection statutes typically seek to regulate the uncontrolled collection, use and dissemination of personal information.[7] Data protection began emerging as a global concern almost forty years ago. While the first data protection legislation was enacted by the German state of Hesse as far back as 1970,[8] promulgation of similar statutes gained momentum with the introduction of 'fair information practices' in the United States and the issuance of principle-based guidelines by the Organisation for Economic Cooperation

5 Yvonne McDermott, 'Conceptualising The Right To Data Protection In An Era Of Big Data' (2017) 4 Big Data & Society 1.

6 Daniel Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; Policy and Research Group of the Office of the Privacy Commissioner of Canada, 'Consent and Privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act' (Office of the Privacy Commissioner of Canada 2016) <https://www.priv.gc.ca/media/1806/consent_201605_e.pdf> accessed 2 June 2018 (Consent and Privacy); Rahul Matthan, Beyond Consent – A New Paradigm for Data Protection, Takshashila Discussion Document, 2017-03 <http://takshashila.org.in/takshashila-policy-research/discussion-document-beyond-consent-new-paradigm-data-protection/> accessed 10 March 2018.

7 '101: Data Protection' (*Privacy International*, 2018) <https://privacyinternational.org/explainer/41/101-data-protection> accessed 9 March 2018.

8 ibid.

and Development ("OECD") in 1980.[9] This section of the paper explores the conceptual foundations and principles that have come to form the bedrock of data protection statutes globally – the principles of notice and consent.[10] It argues that notice and consent are more than mere contractual tools for facilitating the transfer of personal information. As set out more fully below, these principles embody the concept of autonomy and informational self-determination, which are fundamental to the right to privacy.[11]

The impetus to regulating the use of data can largely be attributed to the digitisation of information.[12] As society's use of computers grew, there was a growing need to secure to individuals the right to control information about them.[13] Therefore, the objective of most data protection statutes as set out succinctly in the European Data Protection Directive (the 'EU Directive'),[14] is to protect fundamental rights and freedoms, particularly the right to privacy, while ensuring the free flow of data at the same time.[15] The General Data Protection Regulation (the 'GDPR'), which came into force on 25 May 2018 and repealed the EU Directive, states its objectives in similar terms.[16]

As already stated, privacy as a concept has always been elusive to being defined with any precision. Famously defined as the 'right to be let alone' in Warren and Brandeis' seminal essay,[17] privacy has also been held integral to secrecy, personhood and freedom from surveillance.[18] However, despite undergoing constant evolution in light of newer challenges, there is broad consensus on some of its core elements.[19] One of the most fundamental conceptualisations of privacy is its recognition of autonomy and the right of every individual to make the choices that impact their lives.[20] This includes one's right to

9 Privacy International 2018 (n 7); 'OECD Guidelines on The Protection of Privacy and Transborder Flows Of Personal Data' (*Organisation for Economic Cooperation and Development*, 1980) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm> accessed 9 March 2018.

10 Paul M Schwartz, 'Privacy and Democracy in Cyberspace' (1999) 52 Vanderbilt Law Review 1607, 1614; Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stan Tech L Rev 431,436.

11 Consent and Privacy (n 6); *Puttaswamy Case* (DY Chandrachud J) (n 4).

12 Frits W Hondius, 'A Decade of International Data Protection' (1983) 30 Netherlands International Law Review 103.

13 ibid.

14 Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (EU Directive).

15 EU Directive (n 14), art 1.

16 Council Regulation (EU) 2016/679 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 [2016] OJ L119/1 art 1 (General Data Protection Regulation).

17 Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

18 Solove, 'Conceptualizing Privacy' (n 2).

19 *Puttaswamy Case* (n 4) [102], [118], [127], [320] (DY Chandrachud J).

20 Solove, 'Conceptualizing Privacy' (n 2); Alan Westin (n 3).

control access to, and use of, their personal information. 'Informational self-determination' is, therefore, one of the core guarantees of a right to privacy.[21]

In India, the importance of consent in securing the right to privacy was first recognised by the Supreme Court in *R. Rajagopal v State of Tamil Nadu.*[22] The Court held that publication related to certain kinds of personal information was contingent on prior consent.[23] Subsequently, the Court also went on to recognise consent and autonomy as facets of privacy in the context of a woman's right to make reproductive choices.[24]

In 2017, a nine-judge bench of the Indian Supreme Court delivered its judgment in *K.S. Puttaswamy v Union of India* ('Puttaswamy').[25] This landmark ruling built on the Court's earlier jurisprudence on privacy and unequivocally recognised choice and autonomy as inherent aspects of the right to privacy.[26] The Court located privacy of choice in Articles 19(1)(a) – 19(1)(c) (the right to freedom), Article 20(3) (the right against self-incrimination), Article 21 (the right to life and personal liberty) and Article 25 (the right to freedom of religion).[27] It further held that the right to privacy is not merely a negative right that acts as a restraint on the powers of the state. The positive content of the right imposed an obligation on the state to take all necessary measures to protect the privacy of individuals.[28] This finding becomes important in light of a Committee of Experts having been constituted by the Ministry of Electronics and Information Technology for framing a data protection law in India.[29] As a result of the Supreme Court's ruling, any proposed law must, therefore, strive to give meaning to the autonomy and choice of individuals when asked to part with personal information in return for services.

In the context of data protection, one of the most visible illustrations of informational self-determination is through the principles of notice and consent.[30] Notice requires that the entity collecting personal information (the 'data controller') inform the individual parting with her personal information (the 'data subject') what data it intends to collect, and how

21 Bundesverfassungsgericht, decisions volume 65, p 1(FCC) (The German Census Case); *Puttaswamy Case* (n 4).

22 (1994) 6 SCC 632 [26].

23 ibid. However, the Court did carve out a few notable exceptions, including with respect to public officials and publication based on public records.

24 *Suchita Srivastava v Chandigarh Administration* (2009) 9 SCC 1.

25 (2017) 10 SCC 1.

26 *Puttaswamy Case* (n 4) [248], [297] (DY Chandrachud J), [510] (RF Nariman J.).

27 *Puttaswamy Case* (n 4) [412], [413], [415] (SA Bobde J), [521] (RF Nariman J).

28 Puttaswamy Case (n 4) [326] (DY Chandrachud J).

29 Surabhi Agarwal, 'Justice BN Srikrishna to Head Committee for Data Protection Framework' *The Economic Times* (01 August 2017) <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms> accessed 27 June 2018.

30 McDermott (n 5); Article 29 Data Protection Working Party, 'Opinion 15 / 2011 on the definition of consent' (This Working Party was set up under Article 29 of Directive 95/46/EC, 2011) <http://www.pdpjournals.com/docs/88081.pdf> accessed 2 June 2018; Consent and Privacy (n 6).

it will process it.[31] Similarly, the consent principle stipulates that personal data can only be collected and used pursuant to the data subject's consent.[32] An important corollary to this principle is the power to withdraw consent and opt out from the continued processing of one's personal information.[33]

The rationale for data processing being contingent on informed consent is rooted in empowering the individual to exercise control over the collection, use and storage of her information.[34] Accordingly, consent can only be informed if the notice clearly describes the intended use by the data controller.

Therefore, the relegation of consent to a purely contractual device – that of acceptance of the data controller's offer - is somewhat simplistic in the context of privacy law. Instead, the salience of notice and consent in most modern data protection statutes is indicative of the importance of autonomy as a facet of privacy. This was also recognised by the Supreme Court in *Puttaswamy.*[35]

However, as elaborated below, the extensive use of standard form contracts in the shape of lengthy and complicated privacy notices has led to concerns about the efficacy of a consent-based data protection model.[36] Recent technological developments have complicated this further, leading to growing calls about replacing consent with other principles to effectively secure privacy.[37] The following section of the paper outlines these concerns in greater detail and discusses some of the alternatives that have been put forth.

III. Big Data and Consent Fatigue

Successful implementation of the consent principle is based on the ability of an

31 *Report Of The Group Of Experts On Privacy* (Planning Commission of India 2012) <http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf> accessed 9 March 2018 (Privacy Report 2012).

32 ibid; However, it is useful to clarify that despite the emphasis on consent, it is not the only ground for the processing of personal information. Under most data protection statutes / regulations, processing is permissible if it is necessary for the performance of a contract to which the data subject is a party, or in public interest, among other grounds. See for example, General Data Protection Regulation, art 6.

33 Privacy Report 2012 (n 31).

34 ibid; McDermott (n 5).

35 *Puttaswamy Case* (n 4) (DY Chandrachud J).

36 *Report To The President- Big Data And Privacy: A Technological Perspective* (Executive Office of the President 2014) <https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf> accessed 9 March 2018 (Report To The President).

37 Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) 55 BCL Rev 93; Fred Cate, Peter Cullen and Viktor Mayer Schönberger, *Data Protection Principles For The 21St Century: Revising The 1980 OECD Guidelines* (University of Oxford 2014) <https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf> accessed 9 March 2018; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 Northwestern Journal Technology & Intellectual Property 239.

individual to make an informed decision after reading a privacy notice.[38] This requires that the notice be accessible and easy to understand in terms of setting out the data controller's information practices. However, for several reasons, this has been difficult to achieve.

Most privacy notices are worded in a complicated fashion and usually run into several pages, making it difficult for most people to understand the full import of what they are consenting to.[39] Further, notices are often not available in local languages, preventing a large portion of the population from accessing them.[40]

With the rapid growth of, and reliance on, online services, this accessibility problem has compounded in recent times.[41] Technologically, the advancement of computing power and the steady reduction of storage costs has led to a situation where the retention of data is the norm, and its deletion the exception.[42] Big data – which envisages the use of large data sets to gain unprecedented insights[43] – has, therefore, become a big industry.[44] Big data techniques are particularly intrusive as they enable the creation of detailed profiles from seemingly innocuous and interrelated data.[45] The better part of the last decade has seen tremendous support for the use of big data analytics to facilitate innovation, efficiency and productivity.[46] As a result, both businesses and governments are keen to explore its results to gain greater insights into trends, behaviours and patterns, ostensibly resulting in better targeting of services, products, and policy.[47]

However, big data diminishes the value of consent as it inherently relies on the collection of large amounts of personal data and its continued use for purposes other than what it was

38 Amber Sinha and Scott Mason, 'A Critique Of Consent In Information Privacy' (*The Centre for Internet and Society*, 2016) <https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy#_ftn3> accessed 9 March 2018.

39 Susan E Gindin, 'Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears' (2009) 8 Northwestern Journal Technology & Intellectual Property 1.

40 Sinha and Mason (n 38).

41 Fred H Cate, 'The Limits of Notice and Choice' (University of Hong Kong 2015) <http://www.lawtech.hk/pni/wp-content/uploads/2015/04/Fred-H-Cate.pdf> accessed 14 March 2018; Report To The President (n 36).

42 Viktor Mayer Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press 2010) 52.

43 Crawford (n 37) 96.

44 Tene and Polonetsky (n 37) 243.

45 Crawford (n 37) 98; Viktor Mayer Schönberger and Yann Padova, 'Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation' (2016) 17 The Columbia Science and Technology Law Review 315.

46 James Manyika and others, 'Big data: The next frontier for innovation, competition, and productivity' (McKinsey Global Institute 2011) <http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation> accessed 10 March 2018 (MGI Report); Erik Brynjolfsson, Lorin Hitt and Heekyung Kim, 'Strength in Numbers: How Does Data-Driven Decision-Making Affect Firm Performance?' (April 2011) <http://www.a51.nl/storage/pdf/SSRN_id1819486.pdf> accessed 10 March 2018.

47 MGI Report (n 46).

originally collected for.[48] This information can be used to gain newer insights or make decisions about an individual, giving rise to legitimate concerns regarding discrimination and loss of autonomy.[49]

In view of the unprecedented volume of processing, it is increasingly argued that mandating explicit consent for every use of personal data is no longer practical.[50] Shoe-horning big-data practices into the current regulatory framework has had the unintended consequence of individuals parting with large amounts of personal information pursuant to vague and broadly worded privacy notices.[51]

The growing unease with the centrality of consent within the data protection framework has led to suggestions that the consent principle be replaced with other alternatives. In 2012, Tene and Polonetsky argued that consent and data minimisation principles be 'loosened' in favour of stronger access and transparency rights.[52] They advocated for data processing to be more open to scrutiny, enabling individuals to have more knowledge about how their information was used and how decisions were taken on the basis of it.[53] It was also suggested that giving individuals access to these newer insights would enable them to alter their own choices for the better.[54]

More recently, there have been proposals to replace consent altogether with the principle of accountability.[55] Arguing that the consent model places an unrealistic expectation on individuals to give informed consent for all data use, this proposal, as advocated by Rahul Matthan, seeks to shift the burden of evaluating privacy risks onto the data controller.[56] Accordingly, the accountability principle stipulates that data controllers are responsible for any harm resulting from the data collected or used by them.[57] One particular proposal contemplates strict financial penalties in case of proven 'harm'.[58] Under this model, fiduciary duty over personal data absolves the data controller of seeking consent for its collection and consequently of any restrictions on the uses it can be put to.[59] The proposal is instead based on the right to fair treatment, data security and the right to opt-out, in order to safeguard the rights of individuals.[60] The last guarantee is curious, as despite being

48 Tene and Polonetsky (n 37) 240, 242, 259.
49 Crawford (n 37).
50 Solove, 'Privacy Self-Management and the Consent Dilemma' (n 6); Report To The President (n 36).
51 Viktor Mayer Schönberger and Yann Padova (n 45).
52 Tene and Polonetsky (n 37) 263.
53 ibid 34.
54 ibid 32.
55 Rahul Matthan (n 6); Consent and Privacy (n 6).
56 ibid.
57 ibid. Fred Cate, Peter Cullen and Viktor Mayer-Schönberger, *Data Protection Principles for the 21st Century* (*Maurer School of Law*, 2013) <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1022&context=facbooks> accessed 14 March 2018.
58 Matthan (n 6) 8.
59 ibid.
60 ibid 5-6.

projected as an alternative to consent, the model guarantees a right to opt-out, which is an inherent aspect of consent.

Besides the above, noted privacy scholar Anita Allen has advocated for 'modest paternalism', arguing that in certain circumstances, regulations must bar individuals from waiving their privacy.[61] While Allen acknowledges the dichotomy between favouring individual autonomy and advocating for paternalism in regulation, she justifies her stance by labelling privacy as a 'primary good', essential for dignified co-existence in society.[62]

What emerges from the above is that there is deep unease with the status quo in privacy regulation. There is growing concern that consent ought not to be the sole basis for processing of personal information, as individuals are unable to engage meaningfully with businesses or governments collecting their data. While this concern is legitimate, the above alternatives appear to focus on finding replacements for the consent model, instead of exploring possible methods to strengthen it. The weaknesses of the above proposals and a possible way forward is explored in some detail in the following section.

IV. Why Consent Must Stay

The primary criticism of all these alternatives, as acknowledged by Allan and further articulated by Daniel Solove,[63] is that there is an inherent contradiction in taking away consent in order to safeguard privacy - given that the right serves to enable freedom in decision-making.

The principal issue in favouring accountability over, and instead of consent, stems from the fact that it tends to infantilise the data subject. Irrespective of the practical experience with the consent model, a framework for the protection of privacy based on principles cannot proceed on the basis that individuals are incapable of making meaningful decisions. Here, it is important to create a distinction between the present context and other instances where paternalism is justified – such as mandating seat-belts or helmets for motorists. When the object of the law itself is to protect privacy, the ends cannot be achieved by taking away individuals' autonomy over who accesses their data and how it may be used.

Further, any emphasis on access, transparency or accountability is premised on taking corrective action only *post facto*. That is, both proposed models arm the data subject with rights only after extensive personal information has already been collected and presumably shared with a host of entities. The absence of checks at the time of collection also results in the complete go-by of other essential principles of data protection – that only data that is strictly essential be collected, and that its use be restricted to the purpose it was collected for. In their defence, proponents of the above alternatives envisage this but largely argue that, along with consent, principles of data minimisation and purpose limitation serve to

61 Anita Allen, *Unpopular Privacy: What Must We Hide?* (OUP 2011).
62 ibid.
63 Solove, 'Privacy Self-Management and the Consent Dilemma' (n 6) 1896.

limit the potential of big data.[64]

Besides the above, a more fundamental objection to the entire debate on big data, and consequently the relevance of consent, is that privacy is looked at as an obstacle to the potential advantages of big data.[65] This framing, which pits innovation against privacy, is problematic. Innovation or other related benefits are only desirable if they further individual autonomy, and not if they come at the cost of it.[66]

Accordingly, any articulation of data protection must further individuals' right to autonomy, and give meaning and colour to the Supreme Court's recognition of privacy as a fundamental right. In this context, the recent GDPR serves as an excellent example. Despite being cognizant of recent technological challenges,[67] the framers of the Regulation decided to further strengthen the requirements for valid consent for the processing of personal information.[68] The continuing emphasis on consent in Europe stems from its recognition of protection of personal data as a fundamental right under the Charter of Fundamental Rights of the European Union,[69] and its explicit acknowledgement in the GDPR that 'processing of personal data should be designed to serve mankind.'[70] Therefore, far from doing away with consent, further technological and regulatory safeguards must be introduced to give consent the vigour it requires. However, before attempting to flesh out what these might be, two other clarifications are important.

First, it is a fallacy to view consent as the only basis for processing of personal information. Most data protection statutes, including the GDPR, recognise several other grounds as justification for collection and use of personal information.[71] These include legitimate interests of the controller,[72] processing necessary for compliance with a legal obligation,[73] and public interest.[74]

Similarly, consent should not be allowed to override other mandatory principles of data protection, especially data minimisation and purpose limitation.[75] These are independent

64 Tene and Polonetsky (n 37) 22-23; Matthan (n 6) 242, 259.

65 Submissions by legal academics and advocates to the Justice Srikrishna Committee of Experts on Data Protection (31 Jan 2018) <http://privacyisaright.in/wp-content/uploads/2018/02/Detailed-Answers-to-the-Justice-Srikrishna-Committee-White-Paper-1.pdf> accessed 10 March 2018 (Submissions to White Paper).

66 ibid.

67 General Data Protection Regulation, Recital 6.

68 ibid art 7.

69 Charter of Fundamental Rights of the European Union [2000] OJ C364/01, art 8(1).

70 General Data Protection Regulation, Recital 4.

71 ibid art 6(1).

72 ibid art 6(1)(f).

73 ibid art 6(1)(c).

74 ibid art 6(1)(e).

75 Article 29 Data Protection Working Party, 'Guidelines on Consent Under Regulation 2016/679' (17/EN WP259, 2017) <https://iapp.org/media/pdf/resource_center/wp29_consent-12-12-17.pdf> accessed 13 March 2018.

principles and data controllers must be required to demonstrate compliance with them independent of consent. In other words, privacy notices with broad and vaguely worded purposes should come under scrutiny irrespective of the data subject's consent.

There have been several suggestions for strengthening the existing consent model, all of which deserve due consideration. For instance, Solove recommends adopting partial privacy self – management, where individuals can exercise their consent for the collection and use of their data, but the default option 'nudges' them towards a more privacy-friendly decision.[76] He further suggests that privacy laws forego neutrality in favour of a more value-driven approach – by codifying or classifying certain practices or forms of data collection as being particularly troublesome.[77]

It has also been argued that lawmakers draw from existing safeguards under Indian law, for example under the Contract Act 1872, to supplement the principle of consent with legal rules regarding the validity of a contract.[78] Similarly, the concept of fairness under consumer protection law could also be applied to the data protection context, not just with respect to the terms of the contract, but also in determining how an individual was made to enter it.[79] A related development could also be to mandate a certain degree of granular choice with respect to parting with some kinds of personal information, as opposed to the prevailing 'take it or leave it' approach. This could include an option to the data subject to not part with personal information that is not strictly required by a data controller to provide its product or services.[80] Another means to supplement the consent framework is to mandate a data breach notification mechanism, where, in the event of a data breach and depending on its nature and extent, a data controller would be required to report the breach to the affected data subject(s), allowing them to take necessary corrective action.[81]

The crux of these proposals, therefore, is that the overarching architecture of data protection be strengthened in a manner that facilitates the effective exercise of one's right to consent. This is not merely the correct approach for framing any data protection legislation in India, but also necessary in light of the Supreme Court's landmark decision in *Puttaswamy*. By virtue of the Court locating autonomy within the heart of privacy, and holding that the state had a positive obligation to fulfil this right, the framers of India's data protection law are under an obligation to preserve and strengthen the role of consent in the processing of personal information.

76 Solove, 'Privacy Self-Management and the Consent Dilemma' (n 6).

77 ibid.

78 Smitha Krishna Prasad, 'Back to Basics: Framing a New Data Protection Law for India' (2018). <https://ssrn.com/abstract=3113536 > accessed 10 March 2018.

79 Michiel Rhoen, 'Beyond Consent: Improving Data Protection through Consumer Protection Law' (2016) 5(1) Internet Policy Review <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 10 March 2018.

80 Smitha Krishna Prasad (n 78).

81 General Data Protection Regulation, art 34.

V. Conclusion

The primary focus of this paper has been that the principle of consent must not, and indeed cannot be done away with when formulating principles for a data protection law in India. Consent embodies the concept of autonomy, which is inherent to privacy. With this being expressly recognised by the Indian Supreme Court, the framers of India's data protection law must strive to give it more meaning than it currently has.

However, this paper also acknowledges the legitimate problems with implementing informed consent, especially in light of the widespread use of standard form contracts and the rise of big data. This has given rise to substantial scholarship on the failure of the consent model and several alternatives have been proposed over the last few years.

Nonetheless, as this paper attempts to point out, each of these proposals is not without its flaws. Further, any alternative to consent would entail losing some degree of autonomy over the collection and dissemination of one's personal information. Such a framework would go against the letter and spirit of the Supreme Court's ruling in *Puttaswamy.* Therefore, this paper argues that lawmakers must look to fixing the gaps instead of replacing consent with other alternatives. As outlined above, some of these potential 'fixes' already exist under contract law or consumer protection law and may be moulded appropriately to make India's data protection law more effective. Similarly, a stricter interpretation of free or informed consent can be used to compel data controllers to be more transparent about their data practices, ensuring that data subjects understand what they are consenting to. Regulation could also play a role in mandating data controllers to disclose which information is strictly necessary for the performance of their obligation and which is required solely or largely for advertising purposes.

To conclude, the entire premise of the legislative exercise of drafting a data protection law must be based on the acceptance of a principle-based approach that seeks to enhance citizens' choices. As long as there is a consensus that individual rights and freedoms lie at the centre of a data protection statute, consent will continue to play a vital role.