LET'S MOVE BEYOND CONSENT

- *ARUNIMA BISHNOI*[*]

INTRODUCTION

On August 24, 2017, a nine judge bench of the Hon'ble Supreme Court of India finally upheld the 'Right to Privacy' as a fundamental right, after 67 years of the Constitution's coming into force. It was rightly hailed as a landmark judgment[1] by the privacy enthusiasts and laymen alike. However, in a world of internet, where we 'agree' to hundreds of 'terms and conditions' on a daily basis, without a second thought, the whole idea of privacy stands on a shaky ground. In the process of providing us goods and services, our personal data is being increasingly collected by online service providers, which is further processed and transmitted to third parties and aggregated in the ways that are much beyond our imagination. What we post on social media, which clothes we buy, where we order our food from, when we book our cabs, how much we spend, is all tracked, analysed and correlated to generate more details about our personality and personal lives.[2] Though we can rightfully prevent the government from entering our proverbial castles now, the danger of our sensitive information being misused by the growing number of private e-commerce entities still looms large.

In a welcome move, the central government has set up a panel under the guidance of former Supreme Court judge, Justice B.N. Srikrishna, to suggest a draft of data protection bill to control the actions of non-state parties as well.[3] The bill is expected to have 'user consent' its mainstay[4] as recommended by the nine judges' bench as well as the 'Justice AP Shah Committee Report'[5] framed on the basis of privacy principles adopted

---

[*] Student, Campus Law Centre, Faculty of Law, University of Delhi.

[1] *Justice KS Puttaswamy (Retd) v Union of India* (2017) SCC OnLine SC 996.

[2] Komal Gupta, 'Consent and Privacy Protection' (*Live Mint*, 10 August 2017) <www.livemint.com/Politics/Le4uhieRgGa5PgFiKWH5nM/Why-consent-is-important-in-ensuring-privacy-protection.html> accessed 11 October 2017.

[3] 'Justice Krishna to Head Expert Group on Data Protection Framework for India' (*Press Information Bureau*, 1 August 2017) <http://pib.nic.in/newsite/PrintRelease.aspx?relid=169420> accessed 10 October 2017.

[4] Pankaj Mishra, 'India's Draft Data Protection to Hinge on User Consent; Will be Ready Only Next Year' (*Factor Daily*, 28 August 2017) <https://factordaily.com/india-data-protection-srikrishna-committee/> accessed 12 October 2017.

[5] Planning Commission, '*Report of the Group of Experts on Privacy*' (2012).

throughout the world. According to the consent-based model of data protection (already a smallpart of the Information Technology Act 2000 and its rules),[6] consent of the data subject is required by the data controller to collect, process and use such data for the specified purpose, which ultimately protects it from any consequential liability. On the surface it seems just like the principle behind any other commercial contract, but there is a catch. The problem with consent as a prerequisite for online data collection is, that it's almost never an informed consent, nor even free in many cases and as a result, it has become a mere formality undertaken by the data controllers to safeguard themselves from liabilities, rather than a tool to actively protect the users.

There are many alternative mechanisms that can be deployed in place of consent, and that are already being used effectively by other existing legal regimes. It is the right time for the appointed panel to move beyond 'consent' as the major tool of data protection, and look for some other means that can appropriately replace consent, or, at the least, can be used to supplement it, keeping in mind the socio-economic circumstances of our country.

ORIGINS OF CONSENT IN DATA PROTECTION

To understand the reason behind the importance held by consent, it is essential to know the origins of consent in the field of privacy and data protection. One of the most important factors behind the relevance of consent, seems to be the fact, that data protection has its root in the protection of private property. Many academicians too, acknowledge the relationship between privacy and private property.

History shows that the early parameters of the right to privacy were set in cases involving unconventional property claims in the 18th-century England.[7] In one of the foremost cases, *Pope v. Curl*,[8] a bookseller named Curl obtained and published personal letters written by well-known literary figures without their consent. One of the authors, Alexander Pope, sued Curl, and sought to have the book removed from the market. The judge upheld the privacy of Pope's letters because the author of a letter has a property right over his words.

[6] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[7] Mary Chlopecki, 'The Property Rights Origins of Privacy Rights' (*Foundation of Economic Education*, 1 August 1992) <https://fee.org/articles/the-property-rights-origins-of-privacy-rights> accessed 17 October 2017.

[8] *Pope v Curl* [1741] 2 ATK 342.

In fact, the popular maxim coined by the English jurist, Sir Edward Coke, which is, 'a man's house is his castle',[9] is one of the most significant expressions which highlight's the importance of consent. The 'Castle Doctrine' implies that consent is necessary for preserving property, or else, nobody would be justified in preventing trespass. Similarly, the doctrine of *volenti non fit injuria*, or 'to one who consents, no injury is done', is another articulation of the role of consent in protecting private property. With time, as personal data started to be recognised as part of one's private property,[10] so did consent become an important aspect of privacy protection.

CONSENT UNDER THE INDIAN LAW

Unlike the European Union, India has no legislation focusing exclusively on data protection. The legislative framework regarding the issue of data protection is currently viewed under the lens of the Information Technology Act (hereinafter IT Act),[11] which also applies to other aspects of online regulations, such as e-commerce and cyber-crime. Prior to 2011, the IT Act did not deal with data protection extensively and there were no guidelines on the standard security practices to be adopted by the businesses collecting data online. However, after the European Union enacted stringent laws on data protection, the Indian Government also felt the need for the same, and as a result, a new set of rules called the 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011' were framed. It contains the following major requirements regarding user consent and related issues

PRIVACY POLICY

Rule 4 requires every data controller dealing with sensitive personal data or information (hereinafter SPDI) to publish a privacy policy on its website. The policy must show the type of information collected, the purpose of collecting the information, the procedure of disclosing the information, and the reasonable security practices adopted to safeguard the information.

[9] Adrienne W Fawcett, 'Q: Who Said: 'A Man's Home Is His Castle'?' (*Chicago Tribune*, 14 September 1997) <http://articles.chicagotribune.com/1997-09-14/news/9709140446_1_castle-home-sir-edward-coke> accessed 17 October 2017.

[10] Rohan George, 'Are we Throwing our Data Protection Regime under the Bus?' (*The Centre for Internet and Society*, 29 August 2015) <https://cis-india.org/internet-governance/blog/are-we-throwing-our-data-protection-regimes-under-the-bus> accessed 17 October 2017.

[11] The Information Technology Act 2000.

CONSENT AND NOTIFICATION

Rule 5 requires a data controller to only collect SPDI after obtaining the prior consent of the data subject in writing through a letter, fax or e-mail. Before collecting the information, the business must give the data subject to the option of not providing such information. Further, a user can even withdraw his consent given earlier. In such scenarios, the business has the option to stop providing goods and services for which the information was sought.

DISCLOSURE

According to Rule 6, disclosure of SPDI to a third party is only possible if:

- the data subject has agreed to it through a contract;
- it is necessary to fulfil a legal obligation; or
- the data subject has granted prior permission.

TRANSFER

Rule 7 mandates that a data controller can transfer SPDI to a third party, whether in India or overseas, only if it ensures the same level of protection as that provided under the Indian law. Further, SPDI can only be transferred if it is necessary for the performance of a lawful contract with the data subject, or if the data subject has consented to the transfer.

All the aforementioned rules clearly show that consent is the major and foremost principle governing data protection regulations in India. The security practices required to be adopted by businesses revolve around the pillar of consent. User consent is a pre-requisite for all the transactions involving data - be it collection, disclosure or transfer.

PROBLEMS WITH CONSENT

When the Consent Model was developed, there was an insignificant growth of the Internet, and the entities that collected data were limited. As a result, data could be put to very few uses other than the purpose which it was collected for. After being collected, data used to remain in that organisation itself and was rarely transferred to third parties. It was easier for data subjects to know the details of the data collected and the use which it was being put to. Therefore, it enabled them to make rational choices and give an informed consent for collection and use of data. Analysed in the backdrop of this context, the Consent Model was feasible and adequate.

Fast-forwarding to the current time, unfortunately, that is no longer the case. With data now being collected every time we 'sign up' on a platform, order goods, or pay bills online, it is next to impossible to make a rational choice of allowing someone to use our personal data.

There are numerous issues plaguing the Consent Model, some of which have been analysed below:

LONG AND COMPLEX PRIVACY NOTICES

"*Free consent involves a knowing understanding of what one is doing in a context in which it is actually possible to do otherwise, and an affirmative action in doing something, rather than a mere passive acquiescence in accepting something.*"

- Professor Margaret Jane Radin[12]

But when privacy notices put up by businesses are nothing short of long and complex legal documents drafted by lawyers, full of jargons incomprehensible to a layman, the consent is hardly free or informed. Erik Sherman reviewed about twenty privacy notices put up by e-commerce entities and pointed out that on the first reading, majority of the policies can be understood only by people of a grade level of 15 or above.[13] Although it is not illegal to draft extensive and complex policies, the fact that according to one assessment, a person will at least take 76 working days to evaluate all the privacy policies he/ she has assented to,[14] this should be a serious concern. The major reason behind such complicated terms of use policies is that business organisations want to cover every minute detail possible so that they are absolved of all the liabilities which may be imposed on them in future.[15]

GROWTH OF INTERNET AND EXPANSION OF E-COMMERCE ENTITIES

During the nascent stage of internet, when the data collectors were limited, the user

[12] Margaret Jane Radin, 'Humans, Computers, and Binding Commitment' (2000) 75 ILJ 1125 <www.repository.law.indiana.edu/ilj/vol75/iss4/1/> accessed 11 October 2017.

[13] Erik Sherman, 'Privacy Policies are Great - for PhDs' (*CBS News*, 4 September 2008) <www.cbsnews.com/news/privacy-policies-are-great-for-phds/> accessed 12 October 2017.

[14] Alex Hudson, 'Is Small Print in Online Contracts Enforceable?' (*BBC News*, 6 June 2013) <www.bbc.com/news/technology-22772321> accessed 12 October 2017.

[15] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 NJTIP 239 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364> accessed 10 October 2017.

could make an informed decision of providing his consent based upon the purpose of data collection. Now, with the advent of the Internet of Things, consent is required at every second step the user takes online. When people have to make a huge number of choices, they are bound to ignore the privacy notices and simply go by the default option to 'agree' with them.[16] Such mandatory requirements not only put a substantial obligation on the users but also on the companies seeking consent several times a day[17].

DIMINISHING SCREEN SPACES

When IBM launched the first personal computer in the 1980s, it would not have possibly imagined that one day a 5' screen device would replace it. While the Internet of Things is expanding rapidly, the screens are getting smaller from Personal Computers to Laptops to Smartphones. As the mobile phone interfaces are getting constrained, it is becoming all the more difficult to read and understand privacy notices. In fact, most users do not even read through these several pages long notices on smaller screens.[18] Further, the gen-next equipment such as connected wearable devices (like smart-watches, fitness wristbands, etc.) make sure that privacy notices go absolutely unnoticed. They usually have little or no interface that readily permits choices.

BINARY NATURE OF CONSENT

Another issue plaguing the Consent Model is the binary nature of consent.[19] What is meant by the 'binary nature' is, that a data user has only two choices at his disposal - he can either assent to the lengthy privacy policies, or forego the desired service. This reduces the effectiveness of consent as a powerful tool in the hands of the user to protect his data. When the privacy architects were incessantly toiling day and night to empower individuals to control their data, they had not envisioned this binary choice, which would defeat the very tool designed to protect data.[20] In such a scenario, privacy notices are usually viewed as obstacles that need to be overcome to access the services. On top

[16] Amber Sinha and Scott Mason, 'A Critique of Consent in Information Privacy' (*The Centre for Internet and Society*, 11 January 2016) <https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy> accessed 12 October 2017.

[17] Natasha Singer, 'Mapping, and Sharing, the Consumer Genome' (*The New York Times*, 16 June 2012) <www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all&_r=0> accessed 13 October 2017.

[18] Amber Sinha and Scott Mason (n 16).

[19] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 186 HLR 1880 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018> accessed 14 October 2017.

[20] Fred Cate and *Mayer-Schönberger, 'Notice and Consent in a World of Big Data' (Tech Policy, 26 November 2012) <www.techpolicy.com/NoticeConsent-inWorldBigData.aspx> accessed 14 October 2017.*

of that, consent is required in real time, which leads to users ignoring the privacy notices.[21] As a result, users unknowingly agree to terms and conditions which are unfair to them and prejudicial to their interests.

FALSE ASSUMPTIONS ABOUT THE ROLE OF PRIVACY NOTICES

Research has shown that when people see the phrase 'privacy policy', they tend to assume that the company has proper safeguards in place to ensure the safe handling and protection of their data.[22] Professor Joseph Turow has demonstrated how the use of the term 'privacy policy' leads users to a false assumption that a website which specifically highlights a privacy policy will refrain from sharing their personal data.[23] That's nothing short of a utopian scenario, while the reality is totally different. It is a matter of common knowledge that privacy policies are only meant to protect companies from liabilities, and not to guarantee privacy to users.[24] Data processors can simply shrug off their responsibility by taking advantage of the agreed terms and conditions by the user.

LACK OF AWARENESS ABOUT THE CONSEQUENCES OF CONSENT OR SECONDARY USES OF DATA

In today's interconnected ecosystem of Big Data, ordinary users as well as data collectors often have no idea about what is happening to the data after it is uploaded online.[25] Due to the uncertain and speculative nature of data, the information provided by users transcends the boundaries of 'purpose limitation', and is used for many other purposes apart from what it is collected for. This is because the real value of data comes not from its primary purpose but from its secondary uses.[26] The data provided by users may be aggregated with the data disclosed by them in the past to reveal an otherwise obscure information about their character and personal lives, which can turn out to be overly

[21] Daniel J Solove (n 19).

[22] Chris Hoofnagle and Jennifer King, 'What Californians Understand about Privacy Online' (*SSRN*, 3 September 2008) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130> accessed 14 October 2017.

[23] Joseph Turrow, 'The Trade-off Fallacy', (June 2015) <www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf> accessed 14 October 2017.

[24] Omer Tene and Jules Polonetsky (n 15).

[25] Jonathan Obar, 'Big Data and the Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management' (*SSRN*, 20 August 2015) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239188> accessed 15 October 2017.

[26] Omer Tene, Jules Polonetsky (n 15).

intrusive. However, users have hardly any knowledge about these secondary uses at the time of giving consent, which prevents them from making an informed choice.[27] As observed by De Zwart and others, 'the idea of consent becomes unworkable in an environment where it is not known, even by the people collecting and selling data, what will happen to the data'.[28]

IMPRACTICAL TO OPT-OUT

Earlier, users had a tool to guard themselves against the consequences of giving personal data by opting-out of certain services. It is an important principle of data protection, that, choice of the user is paramount, when it comes to matters involving his personal data. Just as the user has the choice to give consent for the collection of data, he also has the choice to 'opt-out' of data collection (e.g. by stopping the use of a service). However, this concept is being undermined as internet based services are expanding at a rapid pace, and data is being collected in real-time. Opting-out of data collection is becoming increasingly impractical due to the omnipresence of data collection sites.[29] When a user has lost count of the websites where he has provided his personal information, it is next to impossible for him to opt out. Further, so many companies mandatorily require the user to provide data in order to avail their services. This leaves the user with no choice of opting out.

BURDEN ON COMPANIES

The principle of consent is not only disadvantageous to the data users but also to the business entities seeking consent. The responsibility of obtaining consent comes as an additional burden at a time when companies are already withstanding the worst of various legal regulations in the name of 'compliance'. While on the one hand e-commerce entities are focused on improving user experience and ensuring that it is as smooth as possible, on the other hand they are obligated to obtain consent of those very users. It is an extremely difficult job to harmonise the two, as obtaining consent on every stage can lead to quite an unpleasant experience for the user. On top of that, companies are expected to garner consent from disinterested customers by explaining their policies on extremely small screens.[30] Considering all this, it is quite obvious for businesses to

[27] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 186 HLR 1880 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018> accessed 14 October 2017.

[28] Rohan George, 'Are we Throwing our Data Protection Regime under the Bus?' (*The Centre for Internet and Society*, 29 August 2015) < https://cis-india.org/internet-governance/blog/are-we-throwing-our-data-protection-regimes-under-the-bus> accessed 15 October 2017.

[29] Janet Vertesi, 'My Experiment Opting Out of Big Data Made Me Look Like a Criminal' (*TIME*, 1 May 2014) <http://time.com/83200/privacy-internet-big-data-opt-out/> accessed 15 October 2017.

[30] Omer Tene and Jules Polonetsky (n 15).

seek consent for all possible uses, thus giving rise to long and complicated privacy policies.

ALTERNATIVES TO CONSENT

From the aforementioned drawbacks, one can easily see that the current emphasis on consent in data protection seems to be ineffective against illegitimate processing of data in a Big Data context. Not only do uninformed individuals give consent, but also, emphasising on consent may ruin the very purpose of data protection.

It is time to look elsewhere and 'move beyond consent'. Some of the possible alternatives to consent have been analysed below.

RIGHTS MODEL[31]

Any plausible alternative to the Consent Model must make sure that data controllers are held accountable for the harm that they cause to the users, irrespective of whether they obtain prior consent or not. One such alternative is the 'Rights Model', which ensures that the data subjects are not denied the rights over their data, and the data controllers are made liable for any harm to privacy. The model is based upon the following three principles:

ACCOUNTABILITY

Business entities must be held responsible for the data they collect. In addition, if a wrongful loss is caused to the data subject because of processing of data by the collector, the latter must be held accountable for that. The liability must be enforced regardless of any consent given by the subject.

AUTONOMY

Ideally, according to this model, data providers should have complete autonomy over their data. However, since, in the current era of the Internet of Things, it is impossible to prevent collection of data, data subjects should at least have the authority to restrain the ways in which their data is processed.

[31] Rahul Matthan, 'Beyond Consent: A New Paradigm for Data Protection' (*Takshashila Institution*, 20 July 2017) <http://takshashila.org.in/takshashila-policy-research/discussion-document-beyond-consent-new-paradigm-data-protection/> accessed 15 October 2017.

SECURITY

Data collectors are under an obligation to ensure the security of data at all times. They must be held liable for security breach of data even if it does not result into a loss for the data subject.

LEGITIMATE-INTEREST PROCESSING[32]

European privacy laws provide numerous alternatives to consent such as performance of a contract, vital interest of the individuals/public, exercise of official authority, and, most importantly, legitimate interests of the data controller or a third party, provided that rights and freedoms of the individuals are not compromised. 'Legitimate-interest processing' allows the company to process data without consent if there is a rightful and genuine interest of the company or a third party or society in general, in the processing of that data. However, the interest must be real and not too vague. For example, fraud protection, information and network security, improving and marketing products and services, etc., some of which may already be a part of legal compliance. It helps in providing flexibility to businesses to face technological and organisational changes, while requiring them to be proactive and alleviate unfavourable impacts on individuals as they process data.

FOCUS ON RISK AND IMPACT ON INDIVIDUALS[33]

The need to assess and address risks and negative impacts on data subjects is increasingly becoming a legal obligation in various countries. Ranging from formal data privacy impact assessments to deciding relevant security measures, risk is an important consideration while organisations implement their privacy programs. This leads to better protection for individuals, especially in the cases where consent is neither required nor probable.

[32] Information Commissioner's Office UK, 'Guide to Data Protection' (7 July 2017) < https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/> accessed 16 October 2017.

[33] Bojana Bellamy and Markus Heyder, 'Empowering Individuals Beyond Consent' (*IAPP*, 2 July 2015) <https://iapp.org/news/a/empowering-individuals-beyond-consent/> accessed 16 October 2017.

INDIVIDUALS' RIGHTS TO ACCESS AND CORRECTION[34]

Individuals should have the right to access their data and be able to correct it whenever required. It is an essential element of user control that forms an integral part of many privacy regimes. The principle of 'access and correction' also goes on to prove how transparent the functioning of the organisation is.

FAIR PROCESSING[35]

Though, many equate fair processing with providing privacy notices to data subjects, but it goes much beyond that. Fair processing requires the organisations to consider factors such as, whether individuals reasonably expected the proposed use of data, whether processing of data may lead to drawing inferences about individuals, whether individuals were misinformed about the use of their data, what would be the effect of processing on the individuals, etc. These practices help in focusing on the data subjects and protecting them from negative impacts.

STICKY PRIVACY POLICIES[36]

Another alternative for consent is the implementation of a sticky privacy policies regime. This refers to 'machine-readable policies that can stick to data to define allowed usage and obligations as it travels across multiple parties, enabling users to improve control over their personal information'. It mitigates the risk of unforeseeable uses of data because users would not only consent to give data but also to how it would be used afterwards.

RIGHT AGAINST UNFAIR DENIAL OF SERVICE[37]

Many businesses indulge in the unfair practice of requiring individuals to share data

[34] Pranesh Prakash, 'Privacy Laws: Alternatives to Consent' (*Live Mint*, 11 August 2017) <www.livemint.com/Technology/6Bsa8NyF99ZMLb3txybx1J/Privacy-laws-Alternatives-to-consent.html> accessed 16 October 2017.

[35] Information Commissioner's Office UK, 'Big Data, Artificial Intelligence, Machine Learning and Data Protection' (2014) < https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 16 October 2017.

[36] Rohan George, 'Are we Throwing our Data Protection Regime under the Bus?' (*The Centre for Internet and Society*, 29 August 2015) <https://cis-india.org/internet-governance/blog/are-we-throwing-our-data-protection-regimes-under-the-bus> accessed 15 October 2017.

[37] Amber Sinha, 'Rethinking National Privacy Principles' (*The Centre for Internet and Society*, 11 September 2017) <https://cis-india.org/internet-governance/files/rethinking-privacy-principles/view> accessed 16 October 2017.

as a precondition for the provision of services. Everybody should have the right against this denial of services by business entities on the ground of refusing to provide data that is not even essential but only incidental to the provision of services.

CONCLUSION

Though privacy has been upheld as a fundamental right, at a time when more and more people are being connected to the internet and are extensively sharing their personal information for availing services online, it is high time for the Indian government to build a powerful data protection regime. There are many countries to look up to, but care must be taken to not commit the same mistakes made by them, that is, over reliance on the principle of consent.

Consent had been an effective means of protecting privacy and personal data during the emergence of internet. However, in the current era of the Internet of Things and Big Data, consent has not only lost its adequacy, but has also become counter-productive to the very goals of privacy and data protection. As already noted, the long and complex privacy notices provided by businesses produce anything but truly informed consent. Instead of benefitting the users, privacy agreements are mainly drafted for protecting data controllers from unforeseen liabilities. Further, ordinary, uninformed users have hardly any idea about the secondary uses of their data after it is collected, and even if they are made aware of it, opting out of data collection has become nearly impossible. Thus, an overly narrow focus on the necessity of consent deviates our attention from more crucial issues, such as how the data collected is used, modified, shared and repurposed by the data brokers and third parties.

In the backdrop of this context, it is imperative to look for alternatives to consent, or at least for methods that can supplement the 'Consent Model' and make it more effective. The 'Rights Model' seems to be the most suitable and efficacious alternative, wherein data controllers are held liable for all the harms caused to the users regardless of any consent given by them. Companies must be required to consider the risks to data subjects while designing their privacy programs. Not only should there be obligations on data controllers, but also the users should also be provided with rights which ensure a 'meaningful control' over their own data. They must have the right to access and correct their data whenever required, as well as, the right against unfair denial of services for not providing data.

Many privacy regimes, such as the European Union, English and Canadian, have already started exploring and implementing these new models of data protection. India is fortunate for having initiated the formulation of its data protection law at a time when it can take cue from these countries and provide its citizens a powerful tool against illegitimate uses of their data.