CARNEGIE INDIA

WORKING PAPER

MARCH 2020

Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?

Anirudh Burman

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?

Anirudh Burman

This publication was produced under Carnegie India's Technology and Society Program. For details on the program's funding, please visit the Carnegie India website. The views expressed in this piece are solely those of the author.

Carnegie Endowment for International Peace
Publications Department
1779 Massachusetts Avenue NW
Washington, D.C. 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

Carnegie India
Unit C-5 & C-6, Edenpark,
Shaheed Jeet Singh Marg
New Delhi - 110016, India
P: + 011 4008687
CarnegieIndia.org

This publication can be downloaded at no cost at CarnegieIndia.org.

CONTENTS

Introduction

How should a legal framework for data protection balance the imperatives of protecting privacy and ensuring innovation and productivity growth? This paper examines the proposed data protection legislation in India from the perspective of whether it maintains this balance. In December 2019, the government introduced the Personal Data Protection Bill, 2019, in parliament, which would create the first cross-sectoral legal framework for data protection in India.[1]

This paper argues that the bill does not correctly address privacy-related harms in the data economy in India. Instead, the bill proposes a preventive framework that oversupplies government intervention and strengthens the state. This could lead to a significant increase in compliance costs for businesses across the economy and to a troubling dilution of privacy vis-à-vis the state. The paper argues that while the protection of privacy is an important objective, privacy also serves as a means to protecting other ends, such as free speech and sexual autonomy. A framework for protecting personal data has to be designed on a more precise understanding of the role of privacy in society and of the harms that emanate from violations of individual privacy.

The notion of informational privacy has become salient in the past decade but, as this paper illustrates, India has privacy jurisprudence going back several decades. Most of it focuses on privacy in the context of harms caused due to a violation of privacy. This jurisprudence changed in 2017, when the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* held that the Indian Constitution included a fundamental right to privacy.[2] While deciding the case, though the court listed a long line of jurisprudence, the central deficiency in the existing jurisprudence in the court's opinion was the lack of a "doctrinal formulation" that could help decide whether privacy is constitutionally protected.[3]

The jurisprudence on privacy therefore changed—from being valued as a right that protected other ends to being an end in itself. Along with holding that privacy is a fundamental right, the judgment also declared informational privacy to be a subset of the right to privacy.[4] As this paper highlights, this shift is consistent with the approach taken in the bill. The bill aims to protect the informational privacy of individuals by creating a preventive framework that regulates how businesses collect and use personal data, as opposed to protecting informational privacy with a view to the consequent harms caused by the violation of such privacy. In doing so, it focuses primarily on regulating practices related to the use of data.

Not only is this problematic since the proposed framework is unlikely to protect privacy adequately, the bill also significantly strengthens the state's role in the data economy, dilutes property rights in data, and increases state power to surveil without creating adequate checks and balances. This is likely to have deleterious consequences for innovation in the economy while leaving unfulfilled the stated objective of protecting informational privacy.

The first part of this paper provides a summary of the major developments that have led to the demand for a data protection law. It situates the bill in the larger context of India's debate on the right to privacy and problematizes the conception of privacy as outlined in the *Puttaswamy* judgment. This paper argues that the bill follows this new conception of privacy and that in doing so it fails to create a precisely designed regulatory framework that adequately addresses market failures in the digital economy.

The second, third, and fourth parts highlight three key reasons why the bill should be significantly modified. The first is that its reliance on strengthening consent-based mechanisms for protecting personal data is not likely to be effective. A large body of academic work highlights that increased disclosure requirements to users about the use of their data is becoming ineffective in light of modern technological developments. A reliance on such mechanisms could be counterproductive and lead to individuals taking less responsibility while sharing their data.

Second, the preventive framework proposed in the bill could lead to significant compliance costs for private businesses. The bill will regulate data use in all sectors of economic activity and establishes significant new compliance requirements for the vast majority of affected businesses. The costs of compliance will be borne across small and big businesses except those that are specifically exempt. This is problematic since most businesses in India are small. Such compliance requirements would be especially onerous for them. This bill also allows the government to compel businesses to share nonpersonal data with it. This, as the paper argues, could have deleterious consequences for innovation and economic growth in the long run.

The third major issue with the bill is the proposed design of the Data Protection Authority (DPA). This body will be tasked with regulating the provisions of the bill to frame regulations on issues such as mechanisms for taking consent, limitations on the use of data, and cross-border transfer of data. The supervisory mandate of the DPA is sweeping, given the fact that it has to regulate a wide array of preventive obligations, such as security safeguards and transparency requirements, that have to be implemented by businesses.

This broad mandate is being proposed in the larger context of India's generally low regulatory capacity. It is likely that the DPA, therefore, may not be able to either effectively implement the bill or effectively protect informational privacy. This paper argues that, given its cross-sectoral mandate, the DPA may struggle to build internal capacity, leading to either underregulation or overregulation. The former would defeat the intent of the bill while the latter would add unnecessary burdens for compliant businesses. Additionally, the bill does not provide adequate checks and balances to ensure that the central government and the DPA exercise their vast supervisory powers in a reasonable manner.

Lastly, the bill allows the government to exempt any of its agencies from the requirements of this legislation and also allows it to decide what safeguards would apply to their use of data. This, as the paper argues, potentially constitutes a new source of power for national security agencies to conduct surveillance—and, paradoxically, could dilute privacy instead of strengthening it.

The analysis set forth in this paper has been supported by inputs from structured consultations with stakeholders and an empirical analysis of regulatory frameworks in data protection, as well as academic literature on the subject. Participants in roundtables organized by Carnegie India included academics working on privacy, representatives from technology companies and start-ups, and scientific experts. Most participants highlighted specific provisions of the bill that could lead to ineffective regulation or substantial compliance burdens due to the obligations proposed in it. These inputs were corroborated by secondary research, survey reports, and academic literature that highlighted similar issues with data protection regulations in other jurisdictions.

This paper concludes by proposing a framework for modifying the bill and addressing the issues highlighted. In doing so, it argues that there are structural limits to what problems regulation can solve in the data sharing and data processing markets. This is especially true in India, given the extremely low capacity of regulators across sectors. Therefore, data protection legislation must be narrowly focused and designed toward protecting individuals and society against any injury resulting from data processing. A framework designed with this end in mind would achieve a better balance between privacy and innovation.

The Growth of Privacy Regulation and the Bill

The Personal Data Protection Bill, 2019, follows a long line of privacy jurisprudence in India that has been influenced by global developments as well as the country's own constitutional jurisprudence. Though the constitution does not explicitly mention a right to privacy, Indian courts have held that a right to privacy exists under the right to life guaranteed under Article 21.[5] However, there

was always some ambiguity regarding the exact nature of the constitutional protection of privacy due to the long-standing judgment of the Supreme Court in *Kharak Singh v. State of Uttar Pradesh*, where the court held that a right to privacy did not exist under the constitution.[6]

It became necessary to resolve this ambiguity due to two factors that became increasingly relevant: (1) strident claims of loss of privacy in the wake of the government's implementation of its project for unique biometric identification (Aadhaar) and (2) global developments occurring simultaneously.

The growth of the Indian information technology industry and the telecom revolution, which started in the late 1990s, led to the proliferation of digital services in India. This has had two significant consequences. First, the country is increasingly interconnected due to the growth of digital services and platforms.[7] Second, the government has recognized that online service delivery is a powerful vehicle for achieving policy objectives such as financial inclusion and delivering cash transfers. The second objective has been facilitated largely by the implementation of Aadhaar. However, the growing ubiquity of Aadhaar came under sustained criticism from various quarters. One criticism was that Aadhaar was being used for purposes other than social-welfare delivery, such as customer onboarding by private firms. It was alleged that the storage of Aadhaar-related customer information, such as metadata about the place of authentication, constituted a serious breach of privacy.[8] Another significant strain of criticism was that the ubiquity of Aadhaar would enable vastly greater surveillance by the state.

In parallel, the European Union (EU) in 2013 proposed to harmonize and consolidate its preexisting data protection framework through a new regulation: the General Data Protection Regulation (GDPR).[9] The earlier framework was based on the 1995 European Data Protection Directive for protecting personal data.[10] It was felt that this regulatory framework would lead to a fragmented framework of data protection within the EU.[11] The GDPR went through extensive rounds of consultations and finally came into force in 2018. This effort to create a comprehensive data protection regulation in the EU influenced the debate in India.[12]

The debate on the privacy concerns over Aadhaar resulted in a clutch of petitions before the Supreme Court that challenged the validity of the legislation that enabled the system: the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. The five-judge bench of the Supreme Court that heard the petitions stated that, since the petitions claimed infringement of the right to privacy, it was first important to determine whether this right existed under the constitution. It referred this issue to a bench of nine judges of the Supreme Court, which held in August 2017 that a right to privacy did exist under Article 21, that the Supreme Court had decided the question incorrectly in *Kharak Singh*, and that informational privacy was a part of this right to privacy.[13]

The Supreme Court's judgment marked a departure from prior jurisprudence on two grounds. First, it clearly and unambiguously stated that there was a fundamental right to privacy under the constitution. In the context of this paper, however, the more significant ground was that the right to privacy was conceptualized as a right in itself, irrespective of what privacy it helped protect in turn. In a long line of past cases, privacy was used to protect specific interests, such as privacy from nighttime police visits in the *Kharak Singh* case or privacy from telephone tapping in *PUCL v. Union of India*.[14] The Supreme Court's judgment in *Puttaswamy* instead conceptualized privacy as a right worth protecting in itself. This arguably led to a focus away from the actual harm individuals would suffer from a violation of privacy. Importantly, as explained below, this conception of privacy also aligned with already existing regulatory frameworks in data protection in other jurisdictions.

Meanwhile, in July 2017, in response to demands for a comprehensive data protection legislation, the government formed a committee to study issues related to data protection and to propose legislation for it. The committee, chaired by Justice B.N. Srikrishna, published a report laying out the rationale for a legal framework for data protection, as well as a Draft Personal Data Protection Bill, 2018.[15] The report and the draft bill formed the basis of the bill eventually tabled in parliament.

The bill is modeled largely on existing frameworks for protecting privacy in other jurisdictions, including the GDPR and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[16] These regulations themselves are based on older frameworks for the protection of privacy that originated in the 1970s. In 1973, a report of the U.S. Department of Health, Education, and Welfare proposed a set of principles that have been adopted in many countries' privacy frameworks.[17] The "Records, Computers and the Rights of Citizens" report responded to rapid technological developments occurring in the 1970s, specifically computerization and automated processing by government and private firms.[18] Subsequently, the main proposals of the report (such as, no data collection without consent, use limitations, transparency of data processing, and right to correction of data) were adopted by, among others, the Organization for Economic Co-operation and Development.[19]

It is doubtful whether the regulation of data processing based on 1960s technology is relevant in today's age of big data. As early as 1993, an academic, Kenneth C. Laudon, highlighted the limitations of the existing framework. He wrote:

> The FIP [Fair Information Practices] doctrine was based on the technological reality of the 1960s, where a small number of very large-scale mainframe databases operated by the Federal and State governments, or by large financial institutions, were the primary threats to privacy. In this period it was conceivable that an individual could know all the databases in which he or she appeared. But today large scale database systems can be operated by PC based net-

> works (even individual PCs now rival the size of 1960's mainframe capacities). Large scale databases have become so ubiquitous that individuals have no possibility of knowing about all the database systems in which they appear.[20]

If the technological developments of the early 1990s placed the basic principles of data regulation out of sync with market realities, this gap is arguably wider now. For example, the notion of "meaningful consent" is even more problematic than it was in 1993. The bill is, however, based on the same basic principles first set out in 1973.

Major Features of the Bill

The bill provides a legal framework for the collection and use of personal information. In addition to creating a set of rights and responsibilities for the processing of personal data, the bill proposes to create a DPA for making regulations and enforcing the legal framework. The bill also vests substantive standard-setting powers with the central government and tasks the DPA with enforcing the same.

An important feature of the bill is the wide scope of its applicability. If implemented, it will apply to all enterprises across India other than those specifically exempted. This would include any enterprise that uses automated means to collect data. (The DPA will have the power to define small entities based on turnover, volume of data handled, and the purposes of data collection.)[21] This would include not just technology companies and e-commerce platforms, but also real-estate firms and brokers, banking business correspondents, auto dealers, hotels, and restaurants. (For context, the GDPR affects 23 million small businesses in the European Union.)[22] The economy-wide scope of the bill therefore necessitates a close understanding of its provisions and their likely impact.

The bill makes consent a centerpiece of the proposed data protection framework. It proposes that personal data should only be processed on the basis of free, informed, and specific consent, with provisions that allow such consent to be withdrawn. Any data processing without such consent would be a violation and could result in penalties. [23] The bill creates a separate category of "sensitive personal data" and states that such data can be processed only with "explicit consent."[24] Consent has to be taken after giving the user (defined as the "data principal") adequate information about the kinds of data that will be collected and the purposes for which it is being collected.[25] Notice also has to be given regarding the rights and obligations of users and data collectors (defined as "data fiduciaries" in the bill).[26]

The bill provides exemptions from the requirements of notice and consent in certain situations: when performing state functions authorized by law, delivering medical or health services during emergencies or epidemics, and providing services during disasters or the "breakdown of public order." It also contains exemptions from the requirements for "purposes related to employment."[27] In addition, regulations can be made to provide exemptions from consent requirements on grounds such as "prevention and detection of . . . unlawful activity; whistle blowing; mergers and acquisitions; . . . credit scoring; [and] recovery of debt."[28]

The data fiduciary will be required to ensure the data are accurate and stored only for the period necessary for satisfying the purposes of data collection. It also will be accountable for all compliance requirements under the bill.[29] In addition, there are purpose limitations for data use and storage.[30] A consumer can request the data fiduciary to "restrict or prevent the continuing disclosure of personal data" (a matter dealt with in the bill in the right to be forgotten);[31] to give access to certain personal data that it has provided to data fiduciaries in "a structured, commonly used and machine-readable format"; to have it transferred "to any other data fiduciary" (right to data portability);[32] and to correct inaccurate data (right to correction and erasure).[33]

Data fiduciaries have additional obligations, including to implement privacy by design (which requires them to implement business practices that can anticipate, identify, and avoid harms to consumers);[34] to comply with transparency requirements;[35] to create security safeguards—including methods for de-identifying personal data and encryption and steps for preventing misuse of data; and to create grievance-redress systems.[36] "Significant data fiduciaries" have additional obligations. They are required to assess the impact of processing sensitive personal data before processing such data, maintain records regarding "important operations in the data life-cycle,"[37] conduct audits of data processing policies and practices,[38] and appoint data protection officers.[39]

The bill exempts certain kinds of data collection and processing from specific requirements. It states that the central government may exempt "any agency of the government" from "all or any provisions" by passing an order in this regard.[40] In addition, parts of the bill will not apply where data are processed for investigative processes, legal proceedings, domestic purposes, journalistic activities, and statistical and or research purposes.[41] In addition, it proposes partial exemptions for "manual processing by small entities."[42]

The bill requires data fiduciaries to store certain data in India (data localization) and provides an escalating framework for the storage and processing of data based on its sensitivity.[43] It proposes to create three tiers of data with different localization requirements for each—personal data, sensitive

personal data, and critical personal data. Personal data may be transferred freely. The bill makes certain allowances for sensitive personal data to be transferred beyond the country's borders for processing purposes only, as long as the government has granted approval beforehand and as long as users have explicitly given their consent. The bill does not allow critical personal data (as may be defined by the central government) to be transferred outside the country, except on limited grounds and after meeting certain specified conditions.[44]

Monetary penalties are proposed if data fiduciaries fail to comply with certain provisions. These can be as high as "4 percent of the total worldwide turnover of the [data] fiduciary"[45] or a sum of 150 million Indian rupees ($2.1 million), whichever is higher.[46] Lastly, the bill proposes to criminalize activities that lead to the re-identification of individuals. This offense is cognizable—that is, an offense in which an arrest can be made without a warrant—and nonbailable.[47]

The proposed legislation, therefore, adopts a comprehensive preventive framework that applies to varied data collection and usage practices. It creates a number of obligations for businesses that collect and use consumer data and introduces data-related rights for consumers. Since the bill prevents the collection of any personal data without meeting these obligations, it will cover small grocery stores that have fairly uncomplicated data collection practices as well as businesses using sophisticated machine-learning algorithms and large datasets.

The bill will therefore have a significant impact on the economy. India currently has a small number of diversified conglomerates, national and global IT companies, and e-commerce and fintech giants vying for consumers. However, the vast majority of businesses are small businesses. As per the last annual report of the Ministry of Micro, Small and Medium Enterprises, "of the estimated number of 633.92 lakh [63.39 million] enterprises, only 4000 enterprises were large and thereby out of the MSME [micro, small, and medium enterprise] Sector."[48] The overwhelming majority of businesses affected by the bill will be small businesses.

It is therefore important that this bill protects personal data in a manner that protects privacy while allowing for innovation and economic growth. In India, a large majority of the population has become connected to the internet only recently. In a country with poor road, electricity, and communication infrastructure, digital connectivity for this segment of the population is empowering in a manner that is very different than it is for those who are already accustomed to existing in a digital ecosystem. The following sections seek to consider the design and likely impact of the bill in this economic context.

Incorrect Solutions for Online Privacy Harms

Problems With Consent as a Cornerstone of Data Protection

The key regulatory approach adopted in the Personal Data Protection Bill seeks to protect consumers from uses of data that could be harmful to them. The bill does not, however, identify specific harmful practices. Instead, it makes user consent an important part of the data protection framework. In order to do so, it mandates that personal data can only be collected after providing notice and taking consent.[49] Such consent must be free, informed, clear, and specific, and there must be provisions that allow users to withdraw it.[50] In addition, other features such as time limits on data retention and disclosure requirements are intended to regulate how personal data can be used by data fiduciaries. The bill therefore focuses on adequate disclosure to individuals as a mechanism for preventing harm to them.

In addition, the bill aims to reduce the gap in information about the use of personal data between consumers and data fiduciaries. It aims to do so by limiting the purposes of data processing as well as by giving users the right to access their personal data and the right to know how it will be used. Users can also correct their personal data stored with data fiduciaries. The bill requires that data fiduciaries give notice of these rights to consumers before collecting their data.[51] This notice must provide, among other information, purposes for data collection, categories of personal data collected, source of collection, persons with whom such data may be shared, and information about grievance redress.[52]

The proposed DPA will oversee whether data fiduciaries are complying with these obligations.[53]

> The Srikrishna committee regarded these provisions as foundational to the legislation: The notice and choice framework to secure an individual's consent is the bulwark on which data processing practices in the digital economy are founded. It is based on the philosophically significant act of an individual providing consent for certain actions pertaining to her data.[54]

The committee's report states that while consent is the basis for the digital economy, existing practices of consent are broken. Based on this assumption, it proposes to empower the DPA to inquire into cases where the data fiduciaries or processors have "violated any of the provisions of this Act or the rules prescribed."[55]

The report and the bill acknowledge that users are not capable of providing meaningful consent, and yet—somewhat paradoxically—they build on the premise that stronger consent mechanisms can lead to better outcomes.[56] The report argues that consent is usually obtained through complicated agree-

ments that individuals do not read. If they read the agreements, they cannot understand them, and even if the agreements are comprehensible, these agreements cannot be negotiated.[57] But rather than move away from a consent-based framework, the bill incorporates a preventive principle of consent—that is, it concludes that since individuals are incapable of consenting in a meaningful manner, consent must be regulated.

The bill's approach also fails to recognize the ways in which existing legal frameworks that already regulate consent have failed. As stated earlier, since the 1970s, legal frameworks have predominantly been aimed at ensuring consent-based data protection. This legal regime shaped the data collection practices of tech firms that collect personal data. But securing consent has become meaningless as a basis for data protection, not just because of the problems with the idea of meaningful consent but also because sweeping technological changes have rendered the idea even more redundant. It is important, therefore, to ask whether doubling down on a consent-based framework is likely to protect personal data in India.

The Srikrishna committee accepted that consent on the internet is "broken":

> A preponderance of evidence points to the fact that the operation of notice and consent on the internet today is broken. Consent forms are complex and often boilerplate. . . . Any enumeration of a consent framework must be based on this salient realisation: on the internet today, consent does not work.[58]

However, the committee goes on to state that the issue is practical rather than conceptual. In this view, the problem is not with consent per se but how consent-based data protection has been conceived. According to the committee, a better consent architecture is likely to be more effective at protecting privacy.[59] The provisions in the bill, however, do not radically alter existing consent frameworks. They continue to rest on the main assumption that consent is the best mechanism for protecting personal data if supplemented by additional requirements for how it is to be given—explicitly, freely, and capable of being withdrawn.[60]

It is not clear how the Srikrishna committee reached the conclusion that strengthening the consent framework would lead to better data protection. Its report presents no empirical evidence to show how this revised framework would be more effective.

Since the ability to give consent depends on whether a person is knowledgeable about what he or she is consenting to, any empirically grounded consent framework should seek to ascertain how far Indian users value their informational privacy and how they make trade-offs between the benefits of

consenting to digital services and the risks to their privacy.[61] The bill does not base its analysis of this issue on any empirical studies that could answer this question. There is, however, evidence from other jurisdictions that shows that users have a fairly low threshold for consenting to giving away information about themselves.

One study from 2011 found that users of a large software company spent a median time of just six seconds to read the end user license agreement that is part of the process of installing new software.[62] It further found that no more than 8 percent of users bothered to read the license agreement in full.

Similar user behavior has been observed in other studies. An IBM survey found that, though users think companies should be more heavily regulated for data management, 71 percent of them were still willing to give up privacy to get access to the technology they sought, and only 16 percent had ever walked away from a company because of data misuse.[63] Researchers who tracked the online behavior of more than 48,000 visitors to ninety online software companies found that "only 2 out of every 1,000 retail software shoppers access the end-user license agreement [EULAs]."[64] The study found that "EULAs were accessed in only 63 of the 131,729 visits to software retailers (0.05% of all such visits) and in 44 visits to freeware companies (0.15%)."[65] The study goes on to cite research that highlights that increased disclosure is not necessarily likely to increase readership of contract terms.[66]

Other research has found that some users tend to uninstall a software program if they are presented with a notice about a company's data policies with the end user license agreement after they install it. Despite these notices, many users who still opted to download the software later wished that they had not done so.[67]

If users do not use consent agreements to protect their online privacy, should a legal framework enforce a consent-based regime, particularly in the absence of clear evidence that it is likely to work?

In addition, a consent-based framework may instead intensify existing issues. As one paper points out, a consent-and-notice framework designed similarly to the EU's GDPR (as the bill is) is likely to exacerbate the cognitive problems in giving meaningful consent.[68] The Srikrishna committee also noted that users must contend with an overabundance, not a scarcity, of disclosure-related information about consent under existing frameworks.[69] If current consent mechanisms lead to information overload and consent overload, the idea of "stronger" consent proposed in the bill is likely to exacerbate these issues. The proposed framework would therefore provide more information to consumers (consent agreements will have to contain more disclosures and more rights and obligations, and fresh consent will be required for a fresh purpose), without necessarily increasing data privacy.

In addition, the existence of high penalties in the GDPR for violating notice and consent requirements has been critiqued on the basis that it is likely to make technology companies more risk-averse, leading to consent agreements that have stronger opt-in clauses and are even more legalistic in nature.[70] The bill also proposes to impose high monetary penalties for violations.[71] This could work to the detriment of users and companies. Increased consent requirements could lead to increased user desensitization to consent agreements. Firms, meanwhile, may face a situation where users trust them less if they feel they have been misled, even though the firm has complied with legal requirements.[72]

Alessandro Acquisti, a professor of information technology and public policy, points out that an overreliance on consent would create its own costs that could undermine the goals of data protection. He writes:

> Additional costs . . . comprise the social losses due to 'incoherent privacy policies': amidst a complex array of legislative and self-regulatory initiatives, both consumers and firms are uncertain about the level of protection afforded to, or required for, various types of personal data. This uncertainty is costly in itself, in that it forces data subjects and data holders to invest resources into learning about the admissibility of a given data practice. It also creates costly second order effects, in that it may lead both data subjects and data holders to inefficiently under- or over-invest in data protection.[73]

The proposed notice-and-consent framework may therefore be counterproductive. It may not actually prevent harms from online activity but instead exacerbate moral hazard. Users could place increased reliance on regulation and become more careless in their online behavior. Additionally, cognitive loads on users may increase. This could, in turn, make consent requirements futile for protecting personal data. If the proposed notice-and-consent framework is not even going to be able to achieve its stated objective of implementing a preventive privacy framework, its costs for a country like India would outweigh the benefits.

Limitations on Data Processing

The bill proposes various limitations on data processing. These are rooted in the idea that consumers have little knowledge of how their data are being processed. The bill proposes that data should be processed only for specific, clear, and lawful purposes;[74] that the purpose be reasonable;[75] that they be limited to those consented to by users;[76] and that only data that are necessary for such purposes should be collected.[77] In addition, data storage limitations require that data be deleted once the purpose for its collection has been fulfilled.[78]

The rationale behind these requirements is that preventive limits on personal data are likely to result in better individual control over the use of one's personal data and reduce the scope for personal harm. The Srikrishna committee report states:

> If abuse of power is to be prevented, it is critical that the data fiduciary is obliged to use the personal data entrusted to it by the data principal only for the purpose for which the principal reasonably expects it to be used. This is the germ of the collection and purpose limitation principles.[79]

These provisions are agnostic to the kinds of harms that may occur due to the processing of data. Instead of being narrowly tailored toward reducing specific harms, they impose significant preventive obligations with respect to data processing.

However, some of these requirements are at odds with the evolving nature of the digital economy. Compliance with these could lead to productivity losses for India. For one, they seem out of tune with the increased adoption of machine-learning technologies that rely on large datasets to provide services. Big data has been defined as "high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making."[80] The difference between conventional analytics and big data or machine-learning analytics is that "programs don't linearly analyze data in the way they were originally programmed. Instead they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly."[81]

The predictions derived from big data often cannot be foreseen. The "opacity" of data processing, the use of high quantities of data, and "the use of new types of data" are what set big-data analytics apart from conventional ones.[82] Limiting use of data to predefined purposes might hamper such innovations. For example, the Norwegian Data Protection Authority points out that "it is possible that a person's Facebook activities are built into an algorithm that determines whether she will obtain a mortgage from the bank."[83] While such a use may in some cases violate a purpose limitation, it could also benefit potential seekers of credit. A financial service provider with access to such data could potentially reach out to an underserved individual with an offer of credit. In such a case, the benefits of having a purpose limitation would have to be weighed against the costs of the opportunity foregone: increased access to credit. In India, this has important implications for meeting national economic objectives such as financial inclusion.

Additionally, the bill limits the purposes of data collection to those that a user might "reasonably expect."[84] As highlighted earlier, a distinctive feature of big data is the difficulty in understanding how personal data may be used in decisionmaking by algorithms. While the Srikrishna committee report refers to a harms-based test, the bill does not incorporate any such requirement.

Similar concerns have been raised with regard to other provisions of the bill. For example, there is a possibility of conflict between the provision for algorithmic accountability and the use of other emerging technologies such as blockchain.[85] A blockchain is a "digital database containing information that can be simultaneously used and shared within a large decentralized, publicly accessible network."[86] Blockchain technology is increasingly used in businesses such as e-stamping, logistics, and payment systems.[87]

If personal data are stored on blockchain-based databases, such uses would be subject to the requirements of the bill. For example, the bill would require a central node or person to be accountable for the operation of the blockchain as a data fiduciary. However, certain kinds of blockchain designs, such as decentralized blockchains, have no central issuer or controller. The use of such systems could lead to difficulties in how accountability for data processing is assigned.[88] Blockchain is being increasingly used in significant economic sectors in India, such as the TReDS platform for trade invoice discounting and the digitization of land records.[89] While these are largely government platforms, the technology can also be used by private players for protecting intellectual property and enforcing contracts. The provisions of the bill could potentially limit the uses of this technology.

The bill, therefore, seeks to regulate the way technology is used without narrowly identifying harms that could arise from its use. In doing so, it would circumscribe many beneficial uses of emerging technologies.

Alternative Solutions for Protecting Online Privacy

The consent-and-notice framework, as well as the limitations on data processing discussed below, assume that consumer privacy costs under the proposed framework are lower than the benefits of protecting consumer privacy. This may not be the case. First, consumers incur opportunity costs in getting informed about their privacy. For example, there are significant costs to being properly informed about potential risks to privacy by perusing though privacy policies of companies.[90] Second, investment in privacy-enhancing technologies is also a cost for consumers.[91] And third, consumers who prevent their data from being processed forego the benefits that accrue from such processing.

A stocktaking of these costs and benefits would be of great relevance to emerging economies such as India. The government's report on fintech states that the use of emerging technologies, such as artificial intelligence and blockchain, could help address significant issues of access to finance for large sections of society, particularly small businesses.[92]

A country like India—with low levels of access to credit, insurance, and other financial services—may potentially make very different trade-offs between the need for such access on the one hand and the need for informational privacy on the other. By constraining the scope for innovation, the bill arguably overprotects informational privacy at a significant cost to the economy.

The bill does not actually state what harms the provisions on both notice-and-consent and data collection limitations are trying to protect users from. As a result, they are not narrowly tailored toward protecting against harms. Further, they carry a serious risk of restricting innovations that could significantly benefit India.

The argument here is not that data fiduciaries should be allowed to use personal data without consent but rather that regulating consent to protect personal data is not an effective solution. Principles of consumer protection in other economic activities, such as finance, usually prohibit specific kinds of contractual provisions and require the disclosure of specific kinds of activities to consumers. This is narrowly tailored toward the kinds of conduct that could cause harm to consumers.

This regulatory approach is followed in many other sectors. For example, the EU's directive on unfair contractual terms states that

> A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer.[93]

This wide language is constrained by requiring that the unfairness of the contract be assessed "taking into account the nature of goods and services . . . the circumstances attending the conclusion of the contract . . . [and] to all other terms of the contract."[94] This cross-sectoral directive is intended to protect consumers from unfair contractual terms and requires member states to put in place measures to protect consumers from such terms.[95]

To follow this approach, the bill would have to move from a positive to a negative list approach. This would mean that, if users have willingly consented to the use of their data, the privity of such contracts must be respected. There could be certain exceptional circumstances or contractual

provisions that may be deemed too harmful for consumers, and a regulatory agency may be given the power to periodically determine what such terms could be. For the rest, no limitations or liability should be imposed on the use of personal data if consumers have willingly consented to its use.

This would imply that the provisions that require detailed notice and consent would not be required. While data would still have to be processed with user consent, the limitations on purpose, fairness of processing, and data storage would not be required. This approach could potentially have a better chance to protect user privacy in the most cost-effective manner.

New Compliance Costs and their Economic Impact

The preventive approach adopted in the Personal Data Protection Bill is reflected in other provisions that significantly increase compliance requirements for all firms that process data in India. Since "processing" has been defined expansively (for example, also to include the collection of personal data), these requirements would apply to all businesses.[96] However, the costs of these requirements for businesses have not been assessed. The key implications of these provisions for Indian businesses are set out below.

A Significant Increase in Compliance Costs

The bill proposes requirements that all entities processing data will have to comply with. These include data-minimization requirements, notice-and-consent requirements, privacy by design, organizational and management requirements, transparency requirements, security safeguards, localization requirements, and the creation of grievance-redress systems. Significant data fiduciaries would have to implement these and other compliances: data protection impact assessments, appointments of data protection officers, record-keeping requirements, and data audits.

While the bill proposes exemptions for small entities and for certain purposes such as journalistic and research purposes—as well as heightens requirements for significant data fiduciaries—most obligations will be applicable to all businesses, irrespective of the types of risks and the probability of harm involved.

In addition, the bill proposes user rights modeled on the GDPR. Users will have the right to port their data for a fee, seek information on how their data has been used, and have the right to correct it.[97] Users will have the right to ask firms to delete their personal data (that is, they will have the right to be forgotten).[98] Finally, the bill proposes a data localization regime, with tiered restrictions depending on whether the data are merely personal, sensitive personal, or critical personal.[99]

The costs of incorporating these requirements is significant. This has been highlighted by studies on the costs of implementing GDPR requirements for businesses within the EU.[100]

For example, in the United Kingdom, the Ministry of Justice estimated that implementing the GDPR would mean a net annual cost of 220 million British pounds (GBP) to the country in the first year and a total net cost of GBP 2.1 billion in the first fourteen years.[101] Of this amount, the cost of conducting impact assessments were estimated to be between GBP 67 million and 81 million,[102] and the costs of employing a data protection officer for affected firms within the United Kingdom were estimated to range between GBP 60 million and 244 million.[103] The Indian bill has similar requirements, and implementing these would entail significant economic costs in India as well.

A study by the technology firm Cisco on the challenges of implementing the GDPR found that while respondents saw benefits from adopting its requirements, they faced some key challenges, such as meeting data security requirements, changing business processes to meet regulatory requirements, complying with privacy by design requirements, and hiring data protection officers.[104] These challenges are likely to be exacerbated in India, whose economy is poorer and much less digitized compared to the EU.

A checklist published in *A Practical Guide for GDPR Compliance* is a useful indication of the compliance requirements that Indian businesses are likely to face if the bill is enacted.[105] Table 1 provides some key compliance requirements and shows how these will have to be performed by almost all businesses under the bill.

The requirement of data localization could be onerous for Indian businesses. Firms across the economy would have to adopt localization measures to varying degrees, even though no evidence of the economic benefits from such measures has yet been provided. A study from 2014 estimated that developing countries such as Brazil and India would see negative impacts on GDP from any imposition of economy-wide localization measures. This study also estimated that domestic investment in India could see a reduction of up to 1.4 percent due to localization requirements.[106]

The provisions related to localization also have the potential to create significant regulatory uncertainty. The bill proposes that all data classified as critical personal data be stored and processed only in India.[107] Such data can be transferred under certain circumstances if the DPA grants approval or if the government specifically authorizes such transfers.[108] However, since critical personal data has not been defined, this can cause significant uncertainty for businesses that will have to localize personal data.

TABLE 1

Description of Tasks for GDPR Compliance Relevant to India's Personal Data Protection Bill

Description of major compliance requirements under the GDPR	Similar provisions in India's bill
"Review and update current privacy and data protection policies to ensure conformance with the GDPR." "Develop and implement employee training on data protection, the GDPR, and the rights and freedoms of data subjects."	Failure to bring internal policies into compliance with the bill could lead to penalties under S. 57–61. In addition, compensation may be required to be paid under S. 64 to any person who suffers harm as a result of a violation.
"Implement appropriate mechanisms for establishing and receiving consent from data subjects, reflecting the elevated conditions on consent."	S. 11 requires that consent be free, informed, clear, and specific.
"Determine how to collect and store evidence of elevated consent."	S. 11(3) requires that " . . . consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained . . ."
Develop "a method of withdrawing consent, that is just as simple as giving consent."	S. 11(2)(e) requires that data fiduciaries have to ensure that consumers/data principals have the ability to withdraw consent after having given it.
"Develop capabilities for responding to data-access requests by data subjects."	S. 17 provides a right of access.
Notify users "of the right to object to processing, as well as rights of rectification and erasure."	S. 18 provides for the "right to correction and erasure." S. 20 provides for the "right to be forgotten."
"Implement policies and processes for the new requirements under GDPR, such as the rights of data subjects."	Policies will have to be designed to implement Chapter V on "Rights of Data Principal."
"Responding to data-portability requests using an appropriate digital format, and when required, transmitting the requested data directly to the new provider."	S. 19 provides for the "right to data portability."
"Assess the principle of data protection by design and by default against . . . current systems and processes."	S. 22 requires that businesses adopt a privacy-by-design policy.
"Document all data processes and bring them into alignment with GDPR requirements. Keep accurate records of all data processing activities."	Necessary for complying generally with the bill, but also with specific requirements such as purpose limitation requirements under S. 5, collection limitation under S. 6, and fair and reasonable processing requirements under S. 4.
"Appoint a data protection officer."	Required for significant data fiduciaries under S. 30.
"Review data sharing and processing agreements with other organizations, and evaluate their compliance with the provisions of the GDPR." "Review the organizational and technical measures embraced by third parties to protect personal data, and the efficacy of such approaches." "Develop or adopt certification mechanisms or codes of conduct to govern data protection by third-party organizations."	S. 31 regulates how data fiduciaries can outsource data processing activities. S. 10 makes the data fiduciary responsible for "any processing undertaken by it or on its behalf" in the bill.

Description of major compliance requirements under the GDPR (continued)	Similar provisions in India's bill (continued)
"Conduct an end-to-end data inventory and audit, so as to know every location where personal and sensitive personal data is located, processed, stored, or transmitted."	S. 29 requires data audits by significant data fiduciaries.
Monitor "data flows to and from countries outside of the European Union, considering the lawfulness of such transfers under GDPR."	S. 34 regulates cross-border transfers of personal data. All firms that transfer data outside India will be required to comply with this requirement.
"Identify organizational and technical measures that make personal and sensitive personal data inaccessible to the organization, to protect the rights and freedoms of data subjects." Implement "identity management and access control, to ensure only the right people have access to data at the right time."	S. 24 requires data fiduciaries to create security safeguards.
"Keep good records of the organizational and technical measures evaluated and implemented." Ensure ability to "demonstrate actions and mitigations aligned with GDPR compliance when being audited or monitored by a supervisory authority."	S. 49(2)(a) enables the Data Protection Authority to supervise all data protection measures taken by data fiduciaries.
"Establish the lawful basis for each category of data held and associated processing undertaken on such data."	Processing can take place on the basis of consent under S. 11, or one of the grounds mentioned in S. 12-14. The basis for such processing has to be established.
"For services targeted directly at children, establish appropriate practices for verifying data subjects' age and, where necessary, for gaining parental or guardian consent."	S. 16 regulates the collection of children's personal data.
"Implement appropriate policies and notification schemes that will be triggered in the event of a data breach."	S. 25 requires that data fiduciaries inform the DPA of data breaches "where such breach is likely to cause harm to any data principal" and undertake remedial measures.
Develop "automated tools for discovering, cataloguing and classifying personal and sensitive personal data across . . . [the] organization."	The bill also distinguishes between personal data and sensitive personal data, and places different compliance requirements for the same.

SOURCE: For the first column, see see Druva, "A Practical Guide for GDPR Compliance," Osterman Research White Paper, 2017.

Note: In the first column, the author has cited verbatim excerpts from the original table (on pages 9–19 of the white paper) but not the entire original table. The table that appears here should not be interpreted as a full encapsulation of the original table, only a verbatim subset of its findings. In addition, the verbatim excerpts have not been cited in the same order as in the original table. The second column is based on the author's analysis of the Personal Data Protection Bill. Verbatim excerpts from the bill in this column, where used, have been placed within quotes.

Firms would also incur other compliance costs owing to the regulatory requirements imposed by the government and the DPA.[109] Under the bill, all data fiduciaries will have to report their compliance to the authority.[110] In addition, they will have to follow codes of practice framed by the DPA with regard to subjects such as security safeguards and notice and consent.[111] Importantly, the bill allows the government to frame substantive law by allowing it to create additional categories of sensitive personal information.[112] If other categories of sensitive personal information are added, the scope of regulation covered by the bill would increase, adding to compliance costs.

The Expropriation of Nonpersonal Data

The Personal Data Protection Bill provides for the government-mandated sharing of privately collected and developed nonpersonal data. Section 91(2) of the bill states that the government may

> direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

The first element of uncertainty this provision creates stems from its inclusion in a bill ostensibly for protecting personal data. Second, this provision does not indicate the manner in which the government will use such data and does not specify whether businesses mandated to share such data will be compensated for the same. This sanction for forced transfer gives the central government the power to expropriate intellectual property and is likely to have deleterious effects on the incentives for innovation in the long run.[113]

This provision stands in stark contrast to other mechanisms through which the government dilutes intellectual property under other laws. Under the Patents Act, 1970, the government can issue compulsory licenses only if

> "(a) . . . reasonable requirements of the public with respect to the patented invention have not been satisfied, or
> (b) that the patented invention is not available to the public at a reasonably affordable price, or
> (c) that the patented invention is not worked in the territory of India."[114]

Similarly, under the Copyright Act, 1957, the government can issue a compulsory license during the term of copyright only if the owner of the copyright

> "(a) has refused to republish or allow the republication of the work . . . and by reason of such refusal the work is withheld from the public; or

(b) has refused to allow communication to the public by [broadcast] of such work."115

The bill however does not limit the circumstances in which the government can mandate sharing of nonpersonal data. The proactive use or misuse of such powers are likely to reduce incentives for investing in creating nonpersonal data and deriving innovative uses from such data. Lastly, the bill does not require the central government to provide compensation to those who may be required to share nonpersonal data.

The Problematic Conception of "Harm"

The Personal Data Protection Bill seeks to impose regulatory requirements on businesses based on a consideration of whether the use of data is likely to cause harm.[116] However, the definition of "harm" is likely to constitute a significant potential for imposing misdirected compliance costs for businesses and could potentially stifle many legitimate innovative practices.[117]

This is because some of the components of what constitutes harm have no clear underlying rationale. "Any discriminatory treatment" is one such harm.[118] Discrimination is, however, inherent and necessary in a number of business decisions. For example, in the business of giving credit to individuals, public policy should address the legitimate problem of individuals being discriminated against solely on constitutionally protected grounds such as gender or caste. Yet it would be problematic to classify a business decision as a harm if one of these constitutionally protected grounds is combined with other criteria, such as income profile, value of personal assets, and credit history.

It is unclear what forms and types of discrimination the bill seeks to prevent. The constitution recognizes that discrimination is problematic on certain grounds and in certain aspects of public life, such as access to public spaces and employment.[119] The bill does not maintain this balance between the need to legitimately discriminate between consumers and problematic grounds of discrimination.

The bill's definition of harm is used to

- decide the kinds of security safeguards required,
- design "privacy by design" policies,
- classify entities as "significant data fiduciaries,"
- impose penalties on businesses and payment of compensation,
- conduct data impact assessments that have to be done before any new technology is introduced, and
- differentiate between personal and sensitive personal data, among others.

Therefore, not only is the definition of harm overinclusive, it is likely to distort privacy regulation. The definition must be reworded to focus more narrowly on harms that could emanate from the misuse of online data.

For example, in the United Kingdom, the Home Department has prepared a typology of online harms that include cyber bullying, child sexual exploitation, publishing/propagating terrorist content and activity, intimidation, hate crimes, incitement of violence, spreading disinformation, and publishing or posting child pornography.[120] A similar focus on specific harms could reduce compliance requirements while at the same time make privacy-protection requirements more effective.

The Potential Impact on Economic Activity

Section 39 of the bill permits small entities to avoid application of various provisions of the data protection law.[121] But a business can be exempted only if it manually processes data and also meets other conditions specified by the DPA. Thus, a significant number of enterprises will have to comply with the bill's requirements.

The annual report from the Ministry of Micro, Small and Medium Enterprises classifies a micro enterprise in the services sector as one with an annual turnover of 1 million Indian rupees ($14,000).[122] In 2017–2018, most firms in India were classified as micro enterprises.[123] However, the requirement that firms should manually process data means that some of these would not be able to avail of the exemptions.

Many small businesses collect and process personal information in a manner that is incidental to their core business. Such small enterprises would therefore see a significant increase in compliance costs. Even though the bill potentially exempts many businesses from some of the most onerous compliance requirements, they would still have to comply with other requirements including notice and consent, data localization, the right to access, and the correction of individual data.

Larger and more organized firms, especially in the financial and telecommunications sectors, are already subject to regulators' data security and confidentiality requirements. While compliance costs would increase for such firms as well, the magnitude of the increase would be less than that for small businesses that would face large compliance requirements related to data processing for the first time.

The bill could therefore not only increase compliance costs across the economy without necessarily protecting informational privacy, it could also reduce the competitiveness of small businesses. Smaller firms and start-ups would incur significant expenses in proportion to their overall costs in order to meet such compliance requirements.[124]

A stocktaking of the major issues leading to potentially significant compliance costs for Indian businesses highlights the following issues:

- Significant costs arise due to the overarching preventive framework in the bill.
- The proposal to expropriate nonpersonal data is likely to have significantly negative effects on long-term incentives for innovation and could also be challenged as an unconstitutional taking of private property in the absence of a proper framework for compensation.
- The provisions on harms are not narrowly tailored and could distort the regulation of data-related services.

The Amplified Power of the State and the Dilution of Privacy

Strengthening the Supervisory Powers of the State

The Personal Data Protection Bill significantly strengthens the power of the state to regulate the behavior of businesses that collect personal data and, at the same time, grants the Indian government the latitude to allow any government agencies to opt out of complying with the bill's requirements.[125] This has resulted in a paradox where privacy legislation can significantly undermine privacy interests.

The bill proposes to vest the government with significant powers with regard to privacy regulation. For example, the government will have the power to set standards with respect to additional categories of sensitive personal data and voluntary identification methods that social media companies will have to implement.[126]

In addition, its power to exempt any government agency from the provisions of the legislation constitutes a potential dilution of existing safeguards against government surveillance. At present, government surveillance has to take place as per the procedure described under the Telegraph Act, 1885, or the Information Technology Act, 2000.[127]

Under the bill, however, the government will have the power to frame rules regarding "such procedure, safeguards and oversight mechanism to be followed by the agency."[128] This constitutes an independent source of power to create rules regarding surveillance and empowers the government to potentially create different safeguards for different agencies.

The bill also bifurcates the regulation of online businesses between the government and the DPA, and the reason for doing so becomes apparent once the nature of regulatory powers given to each is examined. For example, the government has substantive regulatory powers to regulate social media

intermediaries and require them to implement identity verification mechanisms.[129] They will be treated as significant data fiduciaries and will be required to register with the DPA. It is unclear what privacy concerns are sought to be addressed through these provisions. Identity verification could actually result in the opposite—it could compromise the principle of anonymity on the internet.

The DPA, however, has been given a general mandate to "protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness of data protection."[130]

The bill gives the authority extensive powers to enforce many of the obligations set out. For example, the DPA will have the power to regulate significant data fiduciaries, monitor cross-border transfers of data, and develop mechanisms for creating "data trust scores."[131] For the DPA to perform its functions, the bill proposes that it should have powers to frame regulations, issue directions, seek information, and conduct inquiries.[132]

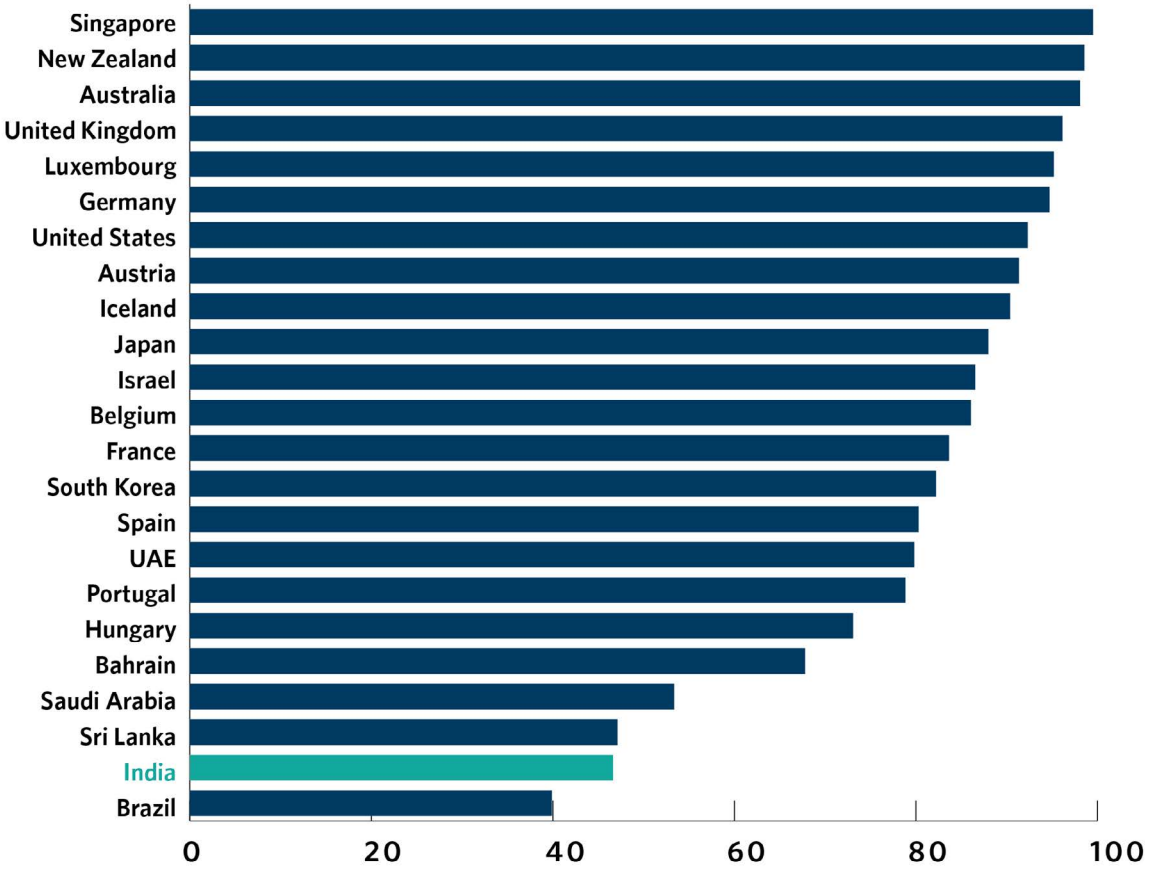
The bill also gives other powers to the authority, including writing regulations to issue codes of practice for subjects such as notice requirements, quality of personal data, manner of obtaining consent, portability, transparency and security requirements, and cross-border transfers.[133] Such codes of practice have to be specified through regulation or by approving codes of practice submitted by industry bodies, statutory authorities, or government agencies.[134] The DPA can exercise these powers only after it has consulted sectoral regulators and other stakeholders in a manner defined by the central government.[135]

To enforce provisions, the authority will have powers to call for information and to inquire into any activity that "is detrimental to the interest of data principals" and to impose penalties for the same.[136] In addition, it will also be vested with the power to search offices and other premises and to seize documents and other information.[137]

The extensive functions and powers given to the government and the DPA amount to a significant addition to the state's powers to regulate online behavior and the practices of businesses that process user data. The government and the DPA are required to ensure a high level of preventive requirements for data protection on the one hand and to address harms and disputes through a wide array of regulatory powers on the other. This is likely to lead to two significant issues: in defining priorities for regulation and capacity building and in the exercise of powers compliant with the rule of law.

FIGURE 1

Ranking of Regulatory Quality Across Countries, 2018



SOURCE: World Bank

The Challenges for Regulatory Capacity

Challenges to the regulation of data emanate from the nature of data itself. Data are nonexhaustible, and the quantity of data being generated from online activity is growing exponentially.[138] In addition, the uses of data are growing rapidly due to technological advancements.[139] This creates problems for regulators. If the quantity and uses of data are increasing at a rapid pace, how do regulatory agencies effectively prevent and redress harms in a field as wide as data protection?

This question is especially relevant for India given its low regulatory capacity.[140] Figure 1, based on a comparison of regulatory quality across multiple jurisdictions highlights this issue.[141] India performs much lower than many other countries with data protection laws in force, such as France, Germany, and the United Kingdom. The functioning of the DPA is likely to be severely constrained given the expansive scope of its mandate under the bill and the generally low regulatory quality of the state.

To fulfil their mandate, the government and the DPA will have to prioritize their objectives. For example, to prevent a specific harm such as a data breach, the authority will have to issue a code of practice to require security safeguards for preventing that harm and monitor compliance as a preventive measure, while also offering remedies in cases where such harm is caused. Given that the DPA's capacity will be finite, its regulatory approach toward focusing on one or the other is likely to be determined by multiple factors: cost-effectiveness, ease with which it can implement the solution, and compliance costs for regulated entities.

However, it would be inherently difficult to determine the correct approach given the high volume of data being generated, the high speed of innovation, and the consequent emergence of new risks, taken together with the cross-sectoral mandate of the DPA.

For example, the authority will have to set standards for methods of deidentification and anonymization requirements and to adjudicate on whether these standards are being complied with. Both these tasks are inherently difficult given the speed and nature of advancements in data processing. The DPA will therefore require a high amount of expertise and sophistication to decide what counts as deidentification and anonymization in a context where new methods of anonymization and reidentification will evolve rapidly.[142]

Sectoral regulators do not face a problem of this scale due to their relatively limited remit.[143] For instance, banking regulators regulate banking entities and intermediaries, and telecommunication regulators narrowly regulate entities within their defined jurisdiction. Their relatively closer linkages to specific markets allows them to formulate regulatory strategies with better information and within a narrower domain. The DPA, however, will regulate the protection of data across multiple sectors without the expert knowledge of the specific contexts of any of them, and it will have to do so in a country with a historically low capacity to regulate well.

This could lead to counterproductive results. In the face of a daunting mandate and low capacity, the DPA may choose to mimic the appearance of effective regulation by enacting a wide number of rules and prescriptions without worrying about outcomes. Lant Pritchett, Matt Andrews, and Michael

Woolcock have called this phenomenon "isomorphic mimicry": a "combination of capability failure while maintaining at least the appearance and often the legitimacy and benefits of capability as 'successful failure.'"[144]

Alternatively, the DPA might choose to signal its effectiveness by using its powers in a draconian manner. Given the wide range of regulatory tools at its disposal and the high ceilings on monetary penalties, it may choose to enforce the law aggressively rather than effectively.[145]

Proper Exercise of Powers by the Government and the DPA

The DPA will have the power to create substantive additional legal requirements (by, for example, defining new types of sensitive personal data and reasonable purposes for data processing). It will also have the power to clarify legal obligations (such as age and consent verification mechanisms, mechanisms and formats for notice and consent, and measures for ensuring transparency and accountability in data protection) and to impose penalties for legal violations.

Given the wide range of powers and functions of the DPA, the institutional framework must ensure that it functions transparently and deliberatively and that it does not abuse its discretion. However, the proposed legal framework does not ensure this.

First, the proposed structure and design of the authority's board does not contain any independent members.[146] Most regulators in India, and globally, have at least some independent members to provide independent inputs and oversight in the functioning of a DPA.

Second, there are inadequate checks and balances on the regulation-framing powers of the government and the DPA. While the bill requires that codes of practice be promulgated only after consultation, it leaves it to the government to prescribe the process to be followed by the DPA for such consultations.[147] The bill does not require the government to follow any such consultative process for its exercise of rule-making powers.

Unlike the United States, India does not have a general administrative framework that requires government agencies to consult with stakeholders.[148] Consequently, Indian regulatory agencies do not usually consult stakeholders while framing regulations.[149] To add to this, judicial review of regulations is usually confined to due-process requirements enumerated in the parent law establishing the agency. If such requirements are absent, courts traditionally defer to the regulatory agencies.[150]

Therefore, in the absence of a provision in the bill that explicitly lays down the consultative process to be followed, the government and the DPA may not follow a regulation-making procedure that is adequately consultative or transparent.

The DPA is therefore likely to be a regulatory agency with severe capacity constraints, highly discretionary powers, and inadequate accountability mechanisms. These design flaws could have a significant effect on the regulatory burden posed on firms across the economy without necessarily protecting informational privacy effectively.

Some of these issues become more significant with respect to the government. The broad power to exempt government agencies from the purview of this bill is extremely problematic, given that the government already has such powers under existing laws. The bill, in creating an independent source of power for state surveillance, increases threats to individual privacy. It is unclear what problem this power is intended to solve. If, however, such exemptions are to be given, the procedure to be followed by government agencies to violate data protection requirements must be stated explicitly in the legislation.

Designing a More Effective Regulatory Framework

Moving to a regulatory approach that focuses primarily on harms arising from contractual terms and that reduces obligations on businesses is likely to reduce the regulatory mandate of the government and the DPA significantly. Further, a pragmatic decision regarding the thresholds for exempting small businesses will enable the DPA to focus its regulatory capacity on a smaller universe of businesses. While this approach does not do away with the intrinsic issues with the regulation of data, it could potentially increase regulatory efficiency.

Even with this reduced scope of regulation, it is essential that the government and the DPA follow a sound regulatory process. To ensure that they do so, the details of the process of framing rules and regulations must be included in the bill.

Conclusion: A More Pragmatic, Privacy-Oriented Approach to Data Protection

To summarize, this paper highlights the following major issues with the Personal Data Protection Bill.

First, the bill requires notice and consent for the collection of data and also places other significant obligations on data processing. These taken together may not actually protect privacy adequately, as

they are based on principles for the regulation of data (fair information practices) devised before the current structure of the market came into existence. These also do not protect users from harms emanating from a violation of privacy. These obligations may instead increase moral hazard and lead to users overestimating the benefits of privacy regulation.

Second, the bill is not based on any empirical understanding of the trade-offs users make while providing their information. The Srikrishna committee, which drafted the first version of the bill, did not undertake any study to assess the specific contexts in which users are willing to exchange personal data for benefits. Evidence from other jurisdictions points to such trade-offs differing depending on the context of the transaction. To the extent that the bill protects privacy without evidence of its relevance to users, it may negatively affect benefits accruing from data-led innovation without effectively protecting personal data.

Third, the bill proposes to impose significant compliance costs on firms engaged in data processing. While small ones are exempt from many obligations, these exemptions will only apply to businesses that manually process data. As a result, a large cross-section of economic actors would have to incur significant costs to implement the bill. The provisions requiring businesses to hand over nonpersonal data to the government are particularly onerous and constitute a significant dilution of property rights. This could have negative long-term effects for innovation and economic growth.

Fourth, "harms" are not well defined. Many of these activities are inherent to many business decisions. The bill's definition of harm could significantly distort the regulation of businesses while not delivering privacy protection.

Fifth, the powers given to the government to exempt government agencies from the bill for the purposes of surveillance constitute a new and independent power to collect personal data. It is unclear why this provision is required, and the bill does not create adequate checks and balances for the use of these powers.

Finally, the design of the DPA suffers from structural issues. The broad preventive framework of the bill will impose serious capacity constraints on it. The proposed composition of the authority does not allow for independent inputs and oversight. The DPA may also not be required to follow adequate consultative processes in its regulation-making functions.

These issues suggest a need for a more pragmatic and modest approach to data protection and harms from misuse of personal data. Since the bill treats privacy as an end, the proposed framework is preventive, all-encompassing, and highly regulated. In doing so, it significantly strengthens the power

of the state to regulate entities that collect data and gives the state additional levers to conduct surveillance. There are obvious limits to the efficacy of protecting privacy through this regulatory design. Instead, the framework should narrowly and precisely focus on problems that can be meaningfully addressed through regulation. The following points enumerate the possible components of such a framework:

1. **Data should not be collected and processed without consent.** Businesses that violate this principle would also violate Indian constitutional norms of informational privacy,[151] as well as the property interests of users. At the same time, consenting individuals must be allowed to take responsibility for their choices.

   Regulation in other consumer-oriented sectors usually takes the form of determining whether certain contractual clauses and practices are unfair, deceptive, or misleading for consumers.[152] The bill should reorient its focus from imposing preventive obligations to identifying and regulating such practices, as well as clauses in data sharing agreements.

   The bill does not adequately protect against specific injuries or harms that can be caused to users. The focus should be on preventing injury to individuals and society that emanate from a breach of data privacy —such as discrimination on constitutionally protected grounds, identity manipulation, financial theft, fraud, and threats to sovereignty and national integrity. This focus on injury prevention must also be used to reformulate the provisions on harms.

   Data fiduciaries should be held accountable for causing injuries of the nature described above. They should, however, not be required to implement preventive measures against all potential misuse of data. Regulation should narrowly address market failures.[153] Reorienting to a narrowly tailored approach would require a shift away from obligations such as privacy by design and appointment of data protection officers.

2. **The remaining preventive regulatory obligations should be layered, based on an assessment of their costs and benefits.** Obligations for firms that do not process data intensively or that do not handle sensitive personal data should be reduced in a manner commensurate to the risks from their activities. One such reduction may be to remove the condition that businesses have to manually process data in order to avail of the exemptions.

3. **Regulatory uncertainty must be reduced.** Ambiguities in the bill must be minimized to improve business certainty. Currently, there are three major issues in the bill that could lead to significant regulatory uncertainty. First, it lacks a sufficiently clear definition of critical personal data. Second, it does not specify criteria for approving cross-border transfers of data. Third, it

gives the government the power to mandate sharing of nonpersonal data without any limitation on the use of this power or details regarding the payment of compensation.

4. **The power given to the government to exempt any government agency from the requirements of the bill should be balanced with adequate safeguards enumerated in the bill itself.** The government should not be given the power to decide which agencies are exempt and the power to decide what safeguards would apply to such agencies.

5. **The mandate given to the DPA should be cognizant of state capacity constraints in India.** The nature of the data economy will make it close to impossible to regulate data processing effectively. The other proposals outlined here can rationalize the scope of the DPA's mandate. For example, the authority would no longer have the mandate to regulate the right to access, the right to be forgotten, and others. In addition, it would not have the mandate to decide how obligations such as purpose limitations are to be implemented. Further, the removal of the ambiguities listed above would provide greater clarity to the DPA on how to implement important provisions of the bill. Finally, raising the threshold—below which firms would be exempt—would significantly reduce the number of businesses subject to the DPA's jurisdiction and enable it to focus on data-intensive businesses.

6. **The DPA and the government should follow a highly consultative process for decisionmaking.** This is considerably more important in this case than for other regulators because of the cross-sectoral applicability of regulations under the bill.

   The bill should accordingly be modified to require the government and the DPA to follow a detailed consultative process for all rules, regulations, and codes of practice they formulate. The Financial Sector Legislative Reforms Commission (2013) proposed a detailed consultative process for financial sector regulators that was enshrined within the legislation itself.[154] This required the board or the apex decisionmaking authority of the regulator to initiate a regulation-making process by first publishing a draft of the proposed regulation, along with a note explaining the reason for the proposed regulation and an analysis of its costs and benefits. It further proposed that all financial sector regulators solicit public comments on the draft and publish a general response to these before framing the final regulation.[155]

   Among other regulators, the Telecom Regulatory Authority of India, the Airports Economic Regulatory Authority, and the Insolvency and Bankruptcy Board of India follow detailed consul-

tative processes before framing regulations. The bill requires the DPA to follow a consultative process. However, this requirement applies only for formulating codes of practice and entrusts the government to prescribe the details of the consultative process.[156] There is a direct link between the thoroughness of the consultative process Indian regulators follow and the specific details of such consultative mechanisms enshrined in the relevant law.[157] The bill should therefore be modified to ensure that the DPA follows best practices in regulation-making for framing regulations and codes of practice.

7. **Lastly, since the functioning of the DPA has an important bearing on the market, its composition should enable it to avail of independent inputs in an institutional manner.** The DPA should have a combination of full-time members and part-time, independent members. Independent members should not be involved in the everyday functioning of the agency. This would allow for independent inputs and a mechanism for external oversight of the agency.

This revised design could enable a more specific and pragmatic framework for protecting the personal data of individuals, while allowing the Indian economy to benefit from innovations in the processing of personal data. As this paper argues, the regulatory framework proposed for protecting the privacy of citizens has to be suitably tailored for the realities of the Indian economy and its regulatory landscape. It is important to have a pragmatic approach to data protection. In the characterization of privacy as an end rather than a means to protect other important societal ends that are specific to India's political economy, the bill significantly strengthens the state without adequately protecting privacy. Designing a more precise and pragmatic regulatory framework can only be done through a pragmatic assessment of the costs and benefits of data protection for India.

About the Author

Anirudh Burman is an associate fellow in the Political Economy Program at Carnegie India.

Acknowledgments

The author is extremely grateful to Suyash Rai, Rudra Chaudhuri, Smriti Parsheera, Ananth Padmanabhan, Upasana Sharma, Arjun Kang Joseph, Aruna Chawla, and Navya Mehrotra for their help and inputs.

Notes

1 All subsequent verbatim quotes from the bill are taken from the following source: India, "Personal Data Protection bill, 2019," Pub. L. No. 373 of 2019, accessed December 16, 2019, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

2 *Justice KS Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012. : https://indiankanoon.org/doc/91938676/?type=print, visited on November 20, 2019.

3 Ibid, at para 91.

4 Anirudh Burman, "Will a GDPR-Style Data Protection Law Work For India?" Carnegie India, August 21, 2019, https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113.

5 See for example, *Govind v. State of Madhya Pradesh* AIR 1975 SC 1378; *R. Rajagopal v. State of Tamil Nadu* AIR 1995 SC 264; *PUCL v. Union of India* AIR 1991 SC 207. *State of Maharashtra v. Madhukar Narayan Mardikar* AIR 1999 SC 495.

6 AIR 1963 SC 1295.

7 "Users in India to Reach 627 Million in 2019," *Economic Times*, accessed November 15, 2019, https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms?from=mdr.

8 Madhav Khosla and Ananth Padmanabhan, "The Aadhaar Challenge: 3 Features That Put Constitutional Rights at Risk," *ThePrint*, June 27, 2018, https://theprint.in/opinion/the-aadhaar-challenge-3-features-that-put-constitutional-rights-at-risk/75576/.

9 European Union, "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)" (n.d.).

10 European Parliament, "Directive 95/46/EC of the European Parliament and of the Council 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," Pub. L. No. Official Journal L 281, 0031 (1995), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

11 European Commission, "Impact Assessment Accompanying the Document - Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," Commission Staff Working Paper, accessed February 11, 2019, https://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF.

12 See for example the comprehensive discussion of the GDPR in the Srikrishna committee, which states, for example, that the committee was informed that the EU was "at the vanguard of global data protection norms." Among other provisions, the report of the committee based its formulation of consent requirements based on the GDPR (page 36). Also see statements of individuals regarding the possible benchmarks for a privacy legislation in India in "Analysis: Data Protection in India—Getting It Right," accessed November 15, 2019, https://www.bankinfosecurity.asia/analysis-data-protection-in-india-getting-right-a-9866. The relevant portion of the analysis states, "Nadkarni suggests that the EU's GDPR would be a good benchmark for India. Poosarla and others also agree that the EU GDPR is a good template to draw from."

13 *Justice KS Puttaswamy v. Union of India*, Writ Petition (Civil) No. 494 of 2012.

14 AIR 1963 SC 1295; and (1997) 1 SCC 301

15 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Draft Personal Data Protection Bill, 2018," accessed March 8, 2019, https://www.thehinducentre.com/resources/article24561526.ece/binary/Personal_Data_Protection_bill,2018_0.
16 "GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules," accessed September 30, 2019, https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/.
17 Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens—Report of the Secretary's Advisory Committee on Automated Personal Data Systems" (U.S. Department of Health, Education & Welfare, July 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.
18 Advisory Committee on Automated Personal Data Systems., 1–12.
19 OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data—OECD," accessed November 15, 2019, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. See also, "A Brief Introduction to Fair Information Practices | World Privacy Forum," accessed November 15, 2019, https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.
20 Kenneth C Laudon, "Markets and Privacy," in *Proceedings of the International Conference on Information Systems*, 1993, 12, https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1025&context=icis1993.
21 Section 39 of the bill.
22 "Millions of Small Businesses Aren't GDPR Compliant, Our Survey Finds," GDPR.eu, May 20, 2019, https://gdpr.eu/2019-small-business-survey/.
23 Sections 11 and 57 of the bill.
24 Section 11 of the bill.
25 Section 7 of the bill.
26 Ibid.
27 Sections 12 and 13 of the bill.
28 Section 14 of the bill.
29 Sections 6, 8, 9 and 10 of the bill.
30 Sections 5 and 6 of the bill.
31 Section 20 of the bill.
32 Section 19 of the bill.
33 Section 18 of the bill.
34 Section 22 of the bill.
35 Section 23 of the bill.
36 Section 24 of the bill.
37 Section 28(1)(a) of the Bill.
38 Section 29 of the Bill.
39 Section 30 of the Bill.
40 Section 35 of the bill.
41 Sections 36 and 37 of the bill.
42 Section 48 of the bill.
43 Sections 40 and 41 of the bill.
44 Section 41 of the bill. The conditions listed for permitted transfers of critical personal data are in section 34(2): "any critical personal data may be transferred outside India, only where such transfer is— (a) to a person or entity engaged in the provision of health services or emergency services where such transfer

is necessary for prompt action under section 12; or (b) to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State."

45 Section 57(2) of the bill.
46 Section 57 of the bill.
47 Sections 82 and 83 of the bill.
48 Ministry of Micro, Small and Medium Enterprises, Government of India, "Annual Report 2017-18 - Ministry of Micro, Small and Medium Enterprises," (New Delhi, India, 2018), https://msme.gov.in/sites/default/files/MSME-AR-2017-18-Eng.pdf., 23.
49 Section 11 of the bill.
50 Section 12(2) of the bill.
51 Section 8 of the bill.
52 Ibid.
53 Section 61(6)(a) of the bill.
54 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018), 32, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf.
55 Section 64(1)(b) of the bill.
56 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," 32.
57 Ibid.
58 Ibid.
59 Ibid., 33–36.
60 Ibid., 33–36.
61 See Alessandro Acquisti, Leslie K. John, and George Loewenstein, "What Is Privacy Worth?," *The Journal of Legal Studies* 42, no. 2 (June 2013): 249–74, https://doi.org/10/gf4gmc. The paper highlights the fact that the trade-offs for consumers between protecting privacy and benefitting from sharing their data varies widely depending on context and the value users perceive from such trade-offs.
62 "MeasuringU: Do Users Read License Agreements?" accessed August 26, 2019, https://measuringu.com/eula/.
63 Erik Sherman, "People Are Concerned About Their Privacy in Theory, Not Practice, Says New Study," *Fortune*, February 25, 2019, https://fortune.com/2019/02/25/consumers-data-privacy/.
64 Yannis Bakos, Florencia Marotta-Wurgler, and David R. Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 1, 2014), https://papers.ssrn.com/abstract=1443256.
65 Ibid., 22.
66 Ibid., 34.
67 Nathaniel S. Good et al., "Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems—CHI '07* (San Jose, CA: ACM Press, 2007), 607, https://doi.org/10/dgc23g.
68 Bart Schermer, Bart Custers, and Simone van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," *Ethics and Information Technology* 16, no. 2 (2014): 19, https://link.springer.com/article/10.1007/s10676-014-9343-8.

69 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," 32.
70 Schermer, Custers, and van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," 9–13.
71 Sections 57-59 of the bill.
72 Schermer, Custers, and van der Hof, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection," 9–13.
73 Alessandro Acquisti, "The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines," in *Joint WPISP-WPIE Roundtable* (OECD, 2010), https://www.oecd.org/sti/ieconomy/46968784.pdf, 14.
74 Section 4 of the bill.
75 Section 5 of the bill.
76 Ibid.
77 Section 6 of the bill.
78 Section 9 of the bill.
79 Committee of Experts under the Chairmanship of Justice B. N. Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna," 53.
80 Information Commissioner's Office, "Big Data, Artificial Intelligence, Machine Learning and Data Protection," accessed August 25, 2019, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, 6.
81 Ibid., 7.
82 Ibid., 9.
83 Datatilsynet—Norwegian Data Protection Authority, "Artificial Intelligence and Privacy," January 2018, https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf, 17.
84 Section 5(b) of the bill.
85 Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR—How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner's Corner," *European Data Protection Law Review (EDPL)* 2 (2016): 422–26, https://doi.org/10/gd247q.
86 "Blockchain," Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/blockchain, visited November 18, 2019.
87 "How Could Blockchain Technology Change Finance," CoinDesk, September 26, 2019, https://www.coindesk.com/learn/blockchain-101/how-blockchain-technology-change-finance.
88 Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR—How to Reconcile Privacy and Distributed Ledgers," Eur. Data Prot. L. Rev. 2 (2016): 424, https://heinonline.org/HOL/LandingPage?handle=hein.journals/edpl2&div=71&id=&page=.
89 Business Line, "India's First Blockchain Implementation Goes Live," April 3, 2018, https://www.thehindubusinessline.com/money-and-banking/indias-first-blockchain-implementation-goes-live/article23422835.ece, accessed on August 20, 2019; and Sharanya Haridas, "This Indian City Is Embracing BlockChain Technology—Here's Why," *Forbes*, accessed August 21, 2019, https://www.forbes.com/sites/outofasia/2018/03/05/this-indian-city-is-embracing-blockchain-technology-heres-why/.
90 Alessandro Acquisti, "The Economics of Personal Data and Privacy: 30 Years After the OECD Privacy Guidelines," in *Joint WPISP-WPIE Roundtable* (OECD, 2010), 18. https://www.oecd.org/sti/ieconomy/46968784.pdf.
91 Ibid., 18.

92 Steering Committee on Fintech Related Issues, *Report of the Steering Committee on Fintech* (New Delhi, India: Department of Economic Affairs, Ministry of Finance, Government of India, 2019), https://dea.gov.in/sites/default/files/Report%20of%20the%20Steering%20Committee%20on%20Fintech.pdf, 31–37.
93 Council of the European Communities, "COUNCIL DIRECTIVE 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts," L 95/29 § (1993), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31993L0013., Article 3(1).
94 Article 4(1) of the Council of the European Communities. (1993).
95 Article 6 of the Council of the European Communities. (1993).
96 Section 3(31) of the bill.
97 Sections 17–20 of the bill.
98 Section 20 of the bill.
99 Sections 33 and 34 of the bill.
100 For a review of the literature, see Burman, "Will a GDPR-Style Data Protection Law Work for India?"
101 Ministry of Justice, United Kingdom, "Impact Assessment: Proposal for an EU Data Protection Regulation," November 22, 2012, https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf, 12.
102 Ibid., 22.
103 Ibid., 23.
104 Cisco, "Maximizing the Value of Your Data Privacy Investments: Data Privacy Benchmark Study 2019," *Cisco Cybersecurity Series*, January 2019, 14.
105 Druva, "A Practical Guide for GDPR Compliance," Osterman Research White Paper, Washington, DC, July 2017, https://go.druva.com/rs/307-ANG-704/images/A%20Practical%20Guide%20for%20GDPR%20Compliance%20-%20Druva.pdf, 9–19.
106 Burman, "Will a GDPR-Style Data Protection Law Work for India?" ; and Matthias Bauer et al., "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper Series, European Centre for International Political Economy, 2014, 10, http://hdl.handle.net/10419/174726.
107 Section 33 of the bill.
108 Section 34 of the bill.
109 Sections 93 and 94 of the bill.
110 Section 49 of the bill
111 Section 50 of the bill.
112 Section 15 of the bill.
113 On the long-run consequences of expropriatory behavior, see, generally: Roderick Duncan, "Costs and Consequences of the Expropriation of FDI by Host Governments," no. 417-2016–26436 (2006): 16, https://doi.org/10/ggfktc. In section six of the paper, the author notes: "This data suggests that countries with past expropriations can expect to have output growth of that mineral almost 6 percent less than countries with no past history of expropriations."
114 Section 84 of the Patents Act, 1970.
115 Section 31 of the Copyright Act, 1957.
116 For example, Sections 22(1)(a) on privacy by design, 24(1) on creating security safeguards, 26(1)(d) on classification of significant data fiduciaries, and 63(4)(a), (b), (g) which include harm as one of the factors to be considered while imposing penalties.
117 Section 3(20) of the bill.
118 Section 3(20)(vi) of the bill. A similar example is "(viii) any denial or withdrawal of a service, benefit or

good resulting from an evaluative decision about the data principal"; see Section 3(21).

119 Article 15 of the Indian constitution.

120 Department for Digital, Culture, Media & Sport, United Kingdom, *Online Harms White Paper*, 2019, 31.

121 The section excludes small entities from application of Sections 8, 9, 10, 24(1)(c), 26, 27, 29-36, 38, and 39 of the bill.

122 Section 7 of the Micro, Small and Medium Enterprises Development Act, 2006, https://indiacode.nic.in/handle/123456789/2013?view_type=search&sam_handle=123456789/1362, visited September 17, 2019.

123 Ministry of Micro, Small and Medium Enterprises, Government of India, "Annual Report 2017-18 - Ministry of Micro, Small and Medium Enterprises," 25.

124 For a discussion on how smaller firms are affected by regulation, see James Bailey and Diana Thomas, "Regulating Away Competition—The Effect of Regulation on Entrepreneurship and Employment," *Mercatus Working Paper*, Mercatus Center, George Mason University, September 2015, https://www.mercatus.org/system/files/Bailey-Regulation-Entrepreneurship.pdf, 11–16.

125 Section 35 of the bill.

126 Section 15 of the bill; and Section 28(3) and (4) of the bill.

127 Section 5 of the Indian Telegraph Act, 1885, accessed December 17, 2019, http://dot.gov.in/act-rules-content/2442; and Section 69 of the Information Technology Act, 2000, https://meity.gov.in/writereaddata/files/The%20Information%20Technology%20Act%2C%202000%283%29.pdf.

128 Section 35 of the bill.

129 Sections 26(4) and 28(3) and (4) of the bill.

130 Section 49 of the bill.

131 Clauses (b), (c), (f), (j) and (k) of section 60(2) of the bill.

132 See sections 49–55 of the bill.

133 Section 49 of the bill.

134 Section 50(2) of the bill.

135 Section 50(4) of the bill.

136 Sections 52 and 53 of the bill.

137 Section 55 of the bill.

138 David Reinsel, John Gantz, and John Rydning, "The Digitization of the World from Edge to Core," 2018, 28, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf. See: "IDC predicts that the Global Datasphere will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025," 3.

139 UNCTAD, "Technology And Innovation Report 2018: Harnessing Frontier Technologies for Sustainable Development" (Switzerland: UNCTAD, 2018), https://unctad.org/en/PublicationsLibrary/tir2018_en.pdf, 4–6.

140 See World Governance Indicators, World Bank, https://info.worldbank.org/governance/wgi/.

141 Table compiled using data for selected countries from World Governance Indicators.

142 Suyash Rai, "A Pragmatic Approach to Data Protection," accessed September 23, 2019, https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html. See section titled "Challenges of building regulatory capacity for data protection."

143 Suyash Rai. See section titled "A unique moral hazard problem." https://macrofinance.nipfp.org.in/PDF/data_protection_comments_suyash.pdf

144 Matt Andrews, Lant Pritchett, and Michael Woolcock, *Looking like a State: The Seduction of Isomorphic Mimicry* (Oxford University Press, 2017), https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780198747482.001.0001/acprof-9780198747482-chapter-3.

145 For a discussion on how the DPA could prefer "form over function" and aggressive enforcement in its functioning, see the section titled "The mandate given to the authority may affect its ability to build capacity," in Rai, "A Pragmatic Approach to Data Protection." https://blog.theleapjournal.org/2018/02/a-pragmatic-approach-to-data-protection.html

146 Section 42 of the bill.

147 See Section 50(4) of the bill.

148 United States, "Federal Administrative Procedure Act" (1946), http://www.law.cornell.edu/uscode/text/5/part-I/chapter-5/subchapter-II.

149 Anirudh Burman and Bhargavi Zaveri, "Measuring Regulatory Responsiveness in India: A Framework for Empirical Assessment," *William and Mary Policy Review* 9 (n.d.): 40, https://www.wmpolicyreview.com/ninepointtwo/2019/4/2/measuring-regulatory-responsiveness-in-india-a-framework-for-empirical-assessment.

150 K. P. Krishnan and Anirudh Burman, "Statutory Regulatory Authorities: Evolution and Impact," in *Regulation in India: Design, Capacity, Performance* (Hart Publishing, n.d.), accessed September 24, 2019, https://carnegieindia.org/2019/04/04/statutory-regulatory-authorities-evolution-and-impact-pub-78780.

151 See, *Justice KS Puttaswamy And Another Vs. Union of India and Ors,* 10 SCC 1 (Supreme Court of India 2017). The Indian Supreme Court held (a) privacy is a fundamental right under the Indian constitution and (b) informational privacy is a subset of the right to privacy protected under the constitution.

152 See for example, the guidance on the issue provided by the UK government: Competition and Markets Authority, "Unfair Contract Terms Guidance—Guidance on the Unfair Terms Provisions in the Consumer Rights Act 2015," Competition and Markets Authority, July 31, 2015, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/450440/Unfair_Terms_Main_Guidance.pdf. The Australian Competition and Consumer Commission follows a similar strategy with respect to consumer protection. See, Australian Competition and Consumer Commission, "Unfair Contract Terms," Text, Australian Competition and Consumer Commission, September 15, 2015, https://www.accc.gov.au/business/business-rights-protections/unfair-contract-terms. In India, the Financial Sector Legislative Reforms Commission proposed this approach in financial consumer protection: see Table of Recommendations 5.5 on page 46 of "Report of the Financial Sector Legislative Reforms Commission," March 2013, http://finmin.nic.in/fslrc/fslrc_index.asp.

153 Financial Sector Legislative Reforms Commission, "FSLRC Report," 11.

154 Financial Sector Legislative Reforms Commission.

155 Financial Sector Legislative Reforms Commission, 31.

156 Section 61 of the bill.

157 Anirudh Burman and Bhargavi Zaveri, "Measuring Regulatory Responsiveness in India: A Framework for Empirical Assessment," William and Mary Policy Review 9 (n.d.): https://www.wmpolicyreview.com/ninepointtwo/2019/4/2/measuring-regulatory-responsiveness-in-india-a-framework-for-empirical-assessment.

CARNEGIE INDIA

United C-5 & 6 | Edenpark | Shaheed Jeet Singh Marg | New Delhi, India 110016 | P: +011 4008687

CarnegieIndia.org