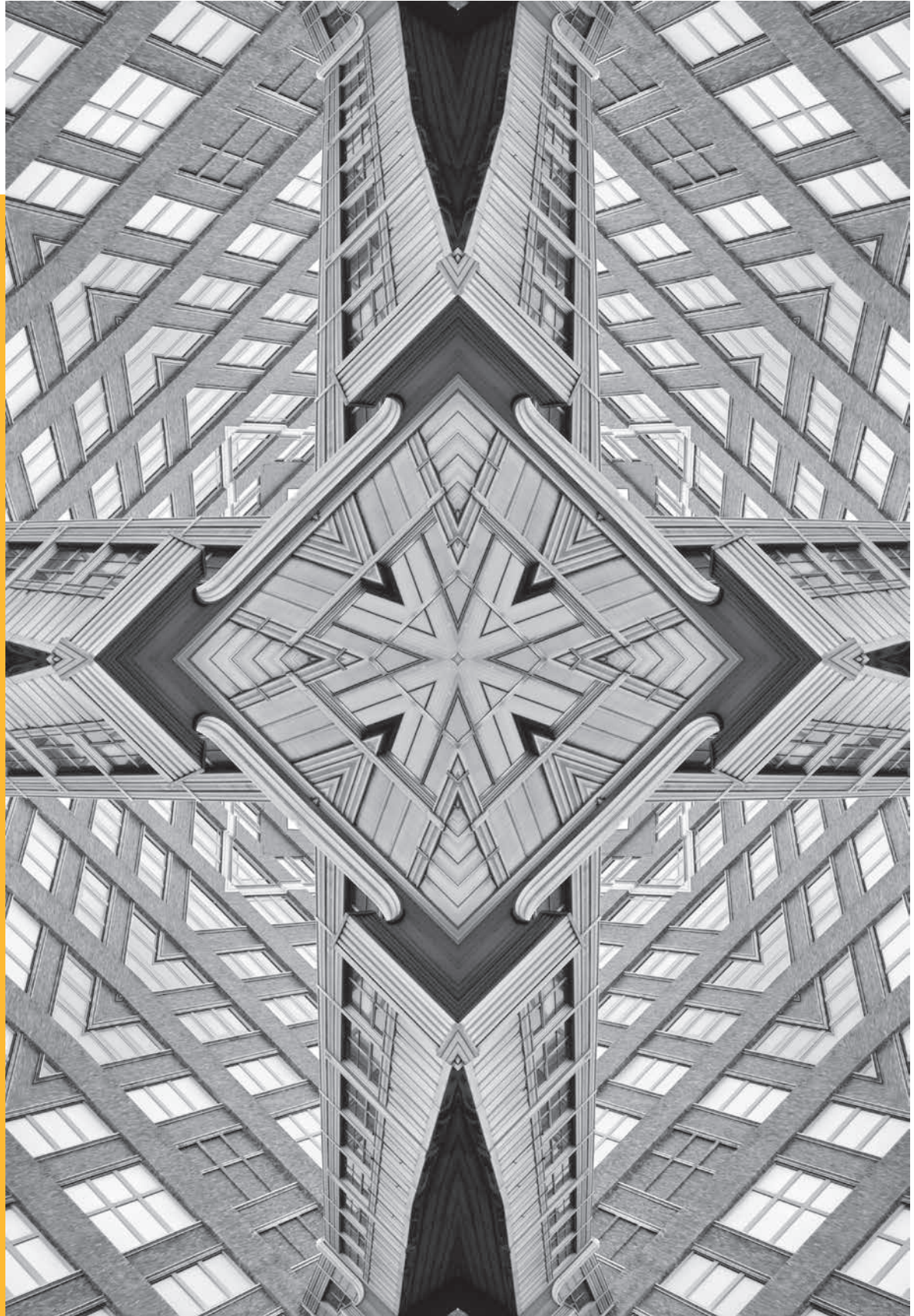


# Occasional Paper



**ISSUE NO. 307 MARCH 2021**

© 2021 Observer Research Foundation. All rights reserved. No part of this publication may be reproduced, copied, archived, retained or transmitted through print, speech or electronic media without prior written approval from ORF.

# A Legal Toolkit for Fair and Competitive Digital Markets in India

**Vikas Kathuria**

## **Abstract**

Ensuring contestability and fairness in India's digital market—one of the world's most prominent—is critical to ensuring consumer welfare. This paper outlines a legal and regulatory framework that can ensure contestability and fairness in the Indian digital market. The paper identifies the following elements of this toolkit: (i) competition law; (ii) ex-ante regulation for digital gatekeepers; (iii) laws for increased transparency in Platform to Business (P2B) transactions; (iv) law on personal data protection; and (v) laws on governing access and sharing of data. The paper makes a case for the adoption of these laws in India, and provides a critique of those laws that have either been adopted or are in the process.

**W**ith a population of 1381.59 million—<sup>1</sup> mostly young, and with expanding purchasing power—India is one of the most lucrative markets in the world. It is the second largest market for mobile phones,<sup>2</sup> and the government is making efforts to develop the market through proactive policies such as ‘Digital India’.<sup>3</sup> Table 1 summarises the magnitude of India’s digital markets.

**Table 1:**  
**India’s Digital Markets: Key Measures**

Parameters	Status	Comments
Internet users	560 million, with Internet penetration of 50%.	Second-highest after China
Smartphone users	760.53 million in 2021, with a penetration of 46.4%.	One of the highest in the world.
E-commerce users	548 million, with a penetration of 40%.	Expected to grow by 61% to 885 million users by 2024.
Social Media users	350 million users, with a penetration of 23.4%	Second-highest after China.

*Source: Author’s own, based on various sources.*

The restrictions in mobility—imposed by the government as a response to COVID-19—have only further accelerated the growth of India’s digital market.<sup>4</sup> In this context, India requires a legal and regulatory framework that can shape and support the growth of its digital economy by ensuring that these markets remain free and fair and thereby work for the benefit of consumers. In such an environment, not only do prices remain low, but market players are able to compete on innovation. Indeed, the digital and economic features of data markets make them prone to concentration and ‘tipping’.<sup>a,5</sup> Additionally, consumer trust is fundamental to the sustainability of any market. The importance of user trust

a ‘Tipping’ refers to the phenomenon when due to network effects a market makes a choice in favour of a particular player once it has gained a critical mass. This is the reason why network industries are usually concentrated with a dominant player at the core. See: <https://www.cs.cornell.edu/home/kleinber/networks-book/networks-book-ch17.pdf>

in data markets is all the more amplified, as user data—which comprises sensitive personal information—is a key determinant of competition and innovation.

This paper outlines the laws that can together ensure that Indian digital markets are strong by ensuring fairness and contestability. In the following sections, the paper provides a brief discussion of five such laws and regulations that together form a legal and regulatory framework to foster a strong Indian digital market by ensuring the twin objective of contestability and fairness.<sup>6</sup> These laws are: (i) competition law; (ii) ex-ante regulation for digital gatekeepers; (iii) laws for increased transparency in Platform to Business (P2B) transactions; (iv) law on personal data protection; and (v) laws on governing access and sharing of data. Some of these laws are already in force, others are under discussion, and still others have fallen off the policy radar.

While discussing each law, the paper also provides international precedents in the respective areas. Most of these laws have originated in the European Union (EU), as it is considered the vanguard of ensuring contestable and fair digital markets through appropriate legal solutions. Taking these laws as a starting point, and drawing lessons from their implementation in those countries, India should strive for contextualisation against its peculiar socio-economic backdrop.

To make the toolkit workable, this paper discusses the laws that have a more direct bearing on competitiveness and fairness in the digital economy. Consequently, laws related to intermediary liability<sup>7</sup> and cybersecurity<sup>8</sup> are not part of this toolkit. Further, as this research is predominantly exploratory in nature, it does not offer an in-depth critique. Each law or regulation forming part of this toolkit merits a separate critique which can be undertaken in future analytical research work.

## 1. Competition Law

*Purpose: To protect and promote competition in digital markets*

*Status: In force*

Theories of mainstream economics propound that markets work best when they are deregulated and players freely compete with one other. This system of rivalry ensures that prices remain low and players bring innovation to the market. Many times, however, a market may be subjected to certain behaviours that may stifle competition: players can enter into agreements to stop competing against each other; or a dominant player can exclude other rivals to reap supranormal profits. Alternatively, mergers between rivals or other players can alter the structure of the market in a way that dampens competition. Competition laws are aimed at ensuring that markets stay contestable and work for the benefit of consumers.<sup>9</sup>

The history of competition laws in India can be traced to 1969 with the enactment of the Monopolies and Restrictive Trade Practices (MRTP) Act. A couple of decades later, changes brought about by liberalisation in the 1990s necessitated a new legislation, and India enacted the new Competition Act in 2002.<sup>10</sup> A new regulator, the Competition Commission of India (CCI) was established on 14 October 2003, but it would only become functional on 20 May 2009.<sup>11</sup>

While competition law has a prominent role to play in all markets, it is an imperative in digital markets that are growing in size and significance. Indeed, tech giants like Facebook,<sup>12</sup> Google,<sup>13</sup> Amazon,<sup>14</sup> and Apple<sup>15</sup> are already facing the power of such laws in the EU, as they stand accused of adversely affecting competition. Some of them are also tackling antitrust cases in the US.<sup>16</sup>

In India, Big Tech firms have faced antitrust scrutiny as well. These investigations are carried out by the CCI, whose actions in digital markets cover online search engines, Online Travel Agents (OTAs),<sup>17</sup> social media platforms,<sup>18</sup> and e-commerce firms.<sup>19</sup> The CCI, for example, has pursued multiple cases against Google. In 2018, Google was fined € 20.42 million for “abusing its dominant position” by preferring its own services over that of the competitors in Google search.<sup>20</sup> In 2019, the CCI ordered an investigation against Google for abusing its dominant position in the licensable Operating System (OS) market by forcing smartphone manufacturers/ Original Equipment Manufacturers (OEMs) to exclusively preinstall Google Mobile Suit (GMS) and bundle the various Google services.<sup>21</sup> In another complaint against Google, the CCI ordered an investigation in November 2020, for abusing its dominant position in the Play Store and Android Operating System (OS), by favouring Google Pay over other competing apps.<sup>22</sup>

Reckoning with the significance of these markets, the CCI in January 2020 released the Market Study on E-Commerce that flagged specific conducts that affect the interest of consumers.<sup>23</sup> Additionally, the CCI is undertaking a market study on mergers and acquisitions in the digital sector to identify such transactions that have the potential of inhibiting future competition in the digital space.<sup>24</sup>

**Comment:** In a span of 11 years, the CCI has developed the capacity to deal with complex cases. However, with respect to digital markets, the CCI understands that these are unique and require “immediate enforcement attention” owing to their economic features and a delay will cause irrevocable harm.<sup>25</sup> Thus, the CCI realises the limitations that the competition law framework faces in these markets.

## 2. Ex-ante regulation for digital gatekeepers

***Purpose: To complement competition law in protecting and promoting competition in digital markets***

***Status: Absent***

Competition law in itself is not enough to ensure that digital markets remain contestable. Owing to the technical and economic features of these markets, by the time a player is subjected to competition law scrutiny, the market has already suffered possibly irreparable harm.<sup>26</sup> Economies of scale including network effects, economies of scope, high entry barriers, lock-in effect, and often, users’ status quo bias—all make it difficult to protect competition. Moreover, traditional remedies have limited efficacy in correcting the market failure in digital markets,<sup>27</sup> and therefore some form of ex-ante regulation is needed.<sup>28</sup>

The CCI seems to favour this solution. In a US-India Business Council virtual roundtable held in July 2020, CCI Chairperson Ashok Kumar Gupta observed:

*These problems are not attributable to the conduct of any one company and are reflected in phenomena such as: (i) excessive concentration in a sector; (ii) high entry barriers; (iii) lack of access to data etc. The incentive to engage in anti-competitive conducts partly arises as the platforms are the ones who determine the rules according to which users, including consumers, business users and providers of complementary services, interact on it. Thus, in digital markets certain business restrictions may be needed to preserve, protect and facilitate competition and to ensure that platform rules do not impede competition without objective justification.<sup>29</sup>*

# Pillars of a Sound Regulatory Framework

The European Commission has come up with a proposal for a Digital Markets Act (DMA),<sup>30</sup> which intends to ensure contestable and fair digital markets through a set of ex-ante regulations for digital gatekeepers. Under the Act, a firm will be designated as ‘gatekeeper’ if it satisfies the following cumulative criteria: it has a strong economic position, a significant impact on the internal market, and is active in multiple EU countries; it has a strong intermediation position, meaning that it links a large user base to a large number of businesses; and, it has (or is about to have) an entrenched and durable position in the market.

The following are some of the salient obligations with which a gatekeeper will have to comply.

- A prohibition on combining personal data of users sourced from different services provided by a gatekeeper unless the user consents to the same. For instance, Google will not be able to combine a user’s data from Google search and those from YouTube, unless the user consents to the same.
- A prohibition on ‘wide’ price parity clauses—also known as Most Favoured Nation (MFN) clauses. This means that online businesses can offer prices or conditions through third-party online intermediation services that are different from those offered through the online intermediation services of the gatekeeper. In the recent past, MFN clauses (both ‘wide’ and ‘narrow’) have been a cause of massive legal uncertainty.<sup>31</sup>
- Allow business users (for instance app developers) to independently provide services to users that have been acquired through the services provided by a gatekeeper (for instance Operating Systems). The CCI has ordered an investigation against Google in similar facts.<sup>32</sup>
- Prohibition on bundling core services of a platform.
- A prohibition on using non-public data of a business user or end-users. This implies that platforms such as Amazon can no longer use the commercially sensitive non-public data of manufacturers and users that can give a competitive edge to Amazon’s own brands. The European Commission in November 2020 sent a Statement of Objections to Amazon on a complaint about using business users’ competitive data.<sup>33</sup>
- A prohibition on preferring a gatekeeper’s own services over that of competitors. In the past, the dual role of platforms has invited several complaints alleging self-preferencing.
- Provide effective data portability facility to end-users.

# Pillars of a Sound Regulatory Framework

- Prohibition on preventing users from un-installing any pre-installed software or app.

While the DMA is at the proposal stage, Germany has moved swiftly and has already incorporated ex-ante regulation in its competition law. The 10<sup>th</sup> Amendment to the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen – “GWB”) introduces a new Sec 19 (a) setting out regulations for “undertakings with paramount significance for competition across markets (UPSCAM)”.<sup>34</sup> As per the amendment, the determination of the “paramount significance for competition across markets” status will depend on the following: a firm’s dominant position on one or more markets; its financial strength or its access to other resources; its vertical integration and its activities on otherwise related markets; its access to data relevant for competition; and, the importance of its activities for third parties’ access to supply and sales markets and its related influence on third parties’ business activities.

The UPSCAM status will stay valid for five years. The German competition agency (the Bundeskartellamt) will prohibit UPSCAM from the following conduct.<sup>35</sup>

- If it engages in self-preferencing when providing access to supply and sales markets.
- Exclusive pre-installation of its own offers on devices or to integrate them in any other way into the undertaking’s offers.
- If it takes measures that hinder other companies in their business activities on procurement or sales markets if the undertaking’s activities are important for access to these markets.
- Directly or indirectly hinder competitors on a market on which the undertaking can rapidly expand its position, even without being dominant.
- If it processes competitively sensitive data collected by the undertaking, to create or appreciably raise barriers to market entry or otherwise hinder other companies, or to require terms and conditions that permit such processing. For instance, if the undertaking makes the use of services conditional on users consenting to the processing of data from other services of the undertaking; or processes competitively sensitive data received from other companies for purposes other than those necessary for the provision of its own services to those companies.



# Pillars of a Sound Regulatory Framework

- If it impedes the interoperability of products or services or the interoperability of data.
- If it provides other companies with insufficient information about the scope, quality or success of the service provided or commissioned.
- If it demands benefits for the treatment of another company's offers that are disproportionate to the reason for the demand.

**Comment:** Similar steps to create an ex-ante regime for powerful digital firms are underway in the United Kingdom (UK), where these regulations have been proposed against firms that have acquired the Strategic Market Status (SMS).<sup>36</sup> Most recently, China has adopted regulations for tech firms.<sup>37</sup> India, being an important digital market, should also move swiftly to ensure that powerful digital firms do not stifle competition.

So far as enforcement is concerned, there can be two models: Either the CCI can be mandated to oversee the regulation of digital markets, just as the German amendment envisions, or a new dedicated regulator can be created for digital markets. The UK Competition and Market Authority (CMA) has opted for the latter model and has proposed the creation of a Digital Markets Unit (DMU).<sup>38</sup>

To be sure, both models have their pros and cons. The first model may benefit from the already gained experience of the antitrust agency and avoid any turf wars with the new digital markets regulator. The second, meanwhile, ensures a dedicated response to digital markets, which requires nuanced understanding of the underlying technology and economics. Moreover, a bifurcated system can also keep a check on a regulator's 'confirmation bias' in ex-post proceedings if a firm escapes negative decisions in ex-ante proceedings.<sup>b</sup>

While adopting ex-ante regulation for digital markets, India should endeavour to strike a balance between the benefits offered by big platforms in the form of network effects, and the potential anti-competitive effects of a platform's practices.<sup>39</sup>

---

<sup>b</sup> It is beyond the scope of this paper to suggest the optimal model in the Indian context.

### 3. Regulations for Increased Transparency in Platform to Business (P2B) transactions

*Purpose: To ensure transparency and trust in Platform-to-Business (P2B) transactions*

*Status: Absent*

As platforms have become more ubiquitous, there is a need to establish trust between them and the businesses they cater to, not only because of the market power they wield, but also the complex nature of the technology involved in their operations. Thus, regulation is required that targets the relationship between online intermediaries and their business users. The EU P2B regulation captures this need in the following recital.

*Online intermediation services can be crucial for the commercial success of undertakings who use such services to reach consumers. To fully exploit the benefits of the online platform economy, it is therefore important that undertakings can trust online intermediation services with which they enter into commercial relationships. This is important mainly because the growing intermediation of transactions through online intermediation services, fuelled by strong data-driven indirect network effects, leads to an increased dependence of such business users, particularly micro, small and medium-sized enterprises (SMEs), on those services in order for them to reach consumers. Given that increasing dependence, the providers of those services often have superior bargaining power, which enables them to, in effect, behave unilaterally in a way that can be unfair and that can be harmful to the legitimate interests of their businesses users and, indirectly, also of consumers in the Union. For instance, they might unilaterally impose on business users' practices which grossly deviate from good commercial conduct, or are contrary to good faith and fair dealing. This Regulation addresses such potential frictions in the online platform economy.<sup>40</sup>*

The focus of the EU P2B regulations is thus to ensure fairness and transparency in these transactions.<sup>41</sup> In turn, ensuring trust in a business-to-business relationship can indirectly improve consumer trust in the online platform economy.<sup>42</sup> The EU P2B regulation applies to online intermediation services and online search engines. Its prominent mandates are the following.

- Providers of online intermediation services are asked to ensure that their terms and conditions are drafted in plain and intelligible language.

# Pillars of a Sound Regulatory Framework

- Providers are required to set out the grounds for decisions to suspend or terminate or impose any other kind of restriction upon, in whole or in part, the provision of their online intermediation services to business users.
- Providers of online intermediation services shall notify, on a durable medium, to the business users concerned about any proposed changes of their terms and conditions. A proper notice period of at least 15 days has to be given to business users before changes are made.
- An intermediation service provider is required to give reasons if it restricts or suspends its services to a particular business user.
- A prominent feature of this legislation is that providers of online intermediation services are required to set out in their terms and conditions the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters.<sup>43</sup>
- Similarly, providers of online search engines are obligated to set out the main parameters, which individually or collectively are most significant in determining ranking and the relative importance of those main parameters.<sup>44</sup>
- Providers of online intermediation services are required to mention any differentiated treatment (and the reasons for the same) provided to any business users in comparison to goods and services provided by itself or any other business user that it controls.
- Where online intermediation services restrict the business users to offer the same goods and services through other means under different conditions, they are required to include the grounds for that restriction in their terms and conditions and make those grounds easily available to the public. Those grounds shall include the main economic, commercial or legal considerations for those restrictions.<sup>45</sup> A case in point is app stores, that have been accused of not allowing the apps to offer better terms through their own websites.<sup>46</sup>

This regulation provides for an internal system for handling the complaints of business users. In case of disputes, the regulation suggests the course of mediation. Business users can also approach judicial bodies to enforce their rights under this legislation.

## Unfair P2B Contract Terms in India

India is the fastest growing market for the e-commerce sector.<sup>47</sup> The E-commerce market study in India also focused on the business users of e-commerce.<sup>48</sup> The report noted that in the category of goods and food services, the majority of sellers and restaurants raised concerns regarding platform neutrality.<sup>49</sup>

The respondents were concerned about a platform preferring its own private label and a set of platforms' "preferred sellers" enjoying preferential treatment from the platforms. The respondents are wary about platforms using sensitive business information to outcompete host businesses on their own platform. Such commercially sensitive data may pertain to price, sold quantities, or demand.<sup>50</sup> Lack of transparency in search ranking was also one of the concerns, as was differential treatment. In particular, sellers and service providers alleged that the commercial terms such as commission rates and penalties for the platforms' own/preferred entities were different from what were offered to other sellers and service providers.<sup>51</sup> Sellers also accused platforms of unilaterally determining and revising the terms of engagement.<sup>52</sup> Some business users of platforms alleged the latter's interference in their pricing sovereignty as some users such as restaurant service providers are forced to offer "deep discounts".<sup>53</sup>

Business users in the food service segment alleged that large platforms bundle delivery service with listing service. This required the restaurants who wanted to list on a platform to also mandatorily register for the platform's delivery services.<sup>54</sup> Restaurants also complained that critical customer information is not shared by platforms with restaurants, while the same is mined for launching and promoting the platforms' own cloud kitchens.<sup>55</sup>

For their part, online travel agencies and online food ordering and delivery platforms alleged the use of "wide"<sup>56</sup> parity provisions in their contracts with, respectively, hotels and restaurants.<sup>57</sup> Several antitrust authorities in the EU have found "wide" parity clauses anti-competitive.<sup>58</sup> Exclusive listing on a particular platform was also brought to the notice in the e-commerce market study of India. Several platforms which operate as pure marketplaces without having their own inventory, were also alleged to be offering discounts over and above the price set by the seller or service provider.<sup>59</sup> Sellers or service providers were apprehensive that platforms use discounts as a discriminatory device.<sup>60</sup>

**Comment:** As mentioned earlier, Indian digital markets have witnessed unfair practices by platforms with respect to their business users. In its e-commerce report, the CCI was of the view that many concerns cited in the study stemmed from information asymmetry, and that by ensuring transparency, such issues could be addressed. To this end, the CCI advocates self-regulation by platforms

vis-à-vis search ranking; collection, use and sharing of data; user review and rating mechanism; revision in contract terms; and discount policy. As it was merely a market investigation by the CCI, it could not make binding recommendations that have the sanction of law. Considering the high stakes for both the platforms and business users (and by implication, the end-users), the government should issue binding regulatory norms for platforms, much like the EU's P2B Regulation.

#### 4. Laws on Personal Data Protection

*Purpose: To ensure users' privacy and security, and create trust in the digital economy*

*Status: In Process<sup>c</sup>*

Any information that can lead to the identification of the individual who generates such information is 'personal data': e.g., names and email addresses, location, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions.<sup>61</sup> This data needs protection as identification may compromise a user's privacy.

The EU General Data Protection Regulation (GDPR),<sup>62</sup> which is the successor of the European Data Protection Directive (1995), that calls for "data protection by design and by default", is the gold-standard for ensuring data protection in the online environment for many jurisdictions. This Regulation came into effect on 25 May 2018. The GDPR comes into play as soon as personal data of EU citizens or residents is processed. It imposes heavy fines, which can go up to € 20 million or 4 percent of global revenue (whichever is higher), if the mandates are not complied with. Also, data subjects can seek compensation for damages.<sup>63</sup>

These are the seven protection and accountability principles that the GDPR mandates: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.<sup>64</sup> The GDPR also recognises these as new privacy rights to accord individuals more control over their data: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling.<sup>65</sup>

<sup>c</sup> At the time of writing this paper, the Bill is with a Joint Parliamentary Committee (JPC) (comprising of members of the Upper House and the Lower House).

# Pillars of a Sound Regulatory Framework

In India, a Committee of Experts led by Justice B.N. Srikrishna was set up in July 2017 to look into the issue of data protection. At present, data protection in India is governed by the Information Technology Act, 2000. Additionally, sectoral laws related to banking, healthcare, and others mandate user privacy. The need for adopting a comprehensive framework was articulated after the Supreme Court of India recognised privacy as a fundamental right<sup>66</sup> that requires stronger protection. The Srikrishna Committee issued its report<sup>67</sup> and also presented the draft Personal Data Protection Bill (PDP), 2018 (revised in 2019). The Committee observed that “[d]ata gathering practices are usually opaque, mired in complex privacy forms that are unintelligible, thus leading to practices that users have little control over.”<sup>68</sup> In India, the PDP Bill aims at safeguarding the privacy of an individual, which has been recognised by the Supreme Court as a fundamental right,<sup>69</sup> while ensuring the growth of the digital economy.

The PDP Bill<sup>70</sup> provides for the protection of personal data of individuals, creates a framework for processing such personal data, and establishes a Data Protection Authority for the purpose.<sup>71</sup> Thus, it gives users control over their data. The Bill distinguishes personal data from *sensitive* personal data and *critical* personal data. The latter category of data has been accorded higher protection,<sup>72</sup> and different categories of data have different data localisation requirements.<sup>73</sup> It also sets out grounds for exemption.

The proposed law covers the processing of personal data by both public and private entities. An entity cannot store or process personal data without the explicit consent of an individual. Some exceptions have been granted. The PDP Bill provides that data can be processed in the following cases: (1) consent, (2) legal obligation, (3) medical emergency involving a threat to life or severe threat to health, (4) providing medical treatment or health services, (5) protecting the safety of individuals during a disaster, (6) employment purposes, and (7) “reasonable purposes” as may be specified by regulations. The Bill has extraterritorial applicability, meaning it would extend to data fiduciaries or data processors not present within the territory of India if they carry out the processing of personal data in connection with personal data of individuals in India.

A separate provision covers the protection of personal and sensitive data of children.<sup>74</sup> Data fiduciaries are required to establish mechanisms for age verification and parental consent. The Bill accords the data principal with the (a) right to confirmation and access, (b) correction and erasure, (c) data portability and (d) right to be forgotten. The Bill also sets out a penalty for non-compliance.<sup>75</sup>

# Pillars of a Sound Regulatory Framework

The PDP Bill also provides for penalties and compensation.<sup>76</sup> Failure to take prompt and appropriate action in response to a data security breach or failure to conduct a data audit is punishable with a fine of INR 5 crore or 2 percent of the annual turnover of the fiduciary, whichever is higher. Failure to adhere to security safeguards or processing of personal data in violation of the Bill is punishable with a fine of INR 15 crore or 4 percent of the annual turnover of the fiduciary, whichever is higher. Re-identification and processing of de-identified personal data without consent is punishable with imprisonment not exceeding three years or with a fine which may extend to INR two lakh, or both.<sup>77</sup> Any data principal who has suffered harm as a result of any violation of any provision under the PDP Bill or the rules or regulations made thereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor.<sup>78</sup>

**Comment:** The draft Bill has attracted criticism on grounds such as the exceptions created for the state, the limited checks imposed on state surveillance, and deficiencies in the structures and processes of the proposed Data Protection Authority.<sup>79</sup> Section 35 of the Bill gives enormous powers to the Central Government to exempt any agency of the Government in respect of the processing of personal data.<sup>80</sup> Another criticism is that the PDP Bill will increase compliance cost by sub-classification of personal data for the purpose of data localisation.<sup>81</sup>

## 5. Laws on governing Access and Sharing of data

*Purpose: To unlock the societal and economic benefits of data sharing*

Data is an essential resource for economic growth, competitiveness, innovation, job creation, and overall societal progress.<sup>82</sup> Data is reusable and non-rivalrous in many cases. Processing of data in combination with data analytics (software), generates information of social and economic value. It can help boost productivity and improve or foster new products, processes, organisational methods and markets.<sup>83</sup> Thus, free-flow in data may give rise to new businesses, foster competition, ensure transparency, and growth in artificial intelligence-driven products/services, resulting in overall welfare.

The Organisation for Economic Cooperation and Development (OECD) estimates that data access and sharing can generate social and economic benefits worth between 0.1 percent and 1.5 percent of gross domestic product (GDP) in the case of public-sector data, and between 1 percent and 2.5 percent of GDP when also including private-sector data.<sup>84</sup>

# Pillars of a Sound Regulatory Framework

While data-sharing may unlock immense benefits, any policy will have to balance these benefits against i) the sensitivity of data and the degree to which personal data could be re-identified; ii) the overlapping rights and interests of all relevant stakeholders; and iii) contributions of various stakeholders in the creation of that data.<sup>85</sup> It is also true that in certain cases, data access and sharing may reduce the producer surplus of data holders.<sup>86</sup>

## Data-Sharing Framework in the EU

The proposed EU Data Governance Act aims to foster the availability of data (both personal and non-personal) for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU.<sup>87</sup> This instrument is aimed to achieve the following.

1. Making public sector data available for re-use, in situations where such data is subject to the rights of others, such as commercial confidentiality, intellectual property, or data protection. Thus, it complements the Open Data Directive<sup>88</sup> (successor of the PSI Directive<sup>89</sup>), which provides common rules for a European market for government-held data (public sector information). There is no obligation though for the public sector bodies.
2. Sharing of data among businesses, against remuneration in any form.
3. Allowing personal data to be used with the help of a ‘personal data-sharing intermediary’, designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR).
4. Allowing data use on altruistic grounds.

Recital 35 of this proposed instrument captures the objective and mechanism through which this instrument aims at making data-sharing possible.

*There is a strong potential in the use of data made available voluntarily by data subjects based on their consent or, where it concerns non-personal data, made available by legal persons, for purposes of general interest. Such purposes would include healthcare, combating climate change, improving mobility, facilitating the establishment of official statistics or improving the provision of public services. Support to scientific research, including for example technological development and demonstration, fundamental research, applied research and privately funded research, should be considered as well purposes of general interest. This Regulation aims at contributing to the emergence of pools of data made available on the basis of data altruism that have a sufficient size in order to enable data analytics and machine learning, including across borders in the Union.<sup>90</sup>*



‘Data altruism’ in the context of this instrument means the consent by data subjects to process their personal data, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services.<sup>91</sup>

## 5.1 Non-personal data-sharing in India

### *Status: In Process*

India understands the potential of non-personal data in ensuring economic and societal progress. The Ministry of Electronics & Information Technology (MeitY) constituted a committee of experts in September 2019, under the leadership of Kris Gopalakrishnan to look at non-personal data-sharing framework in India. While constituting the Committee, MEITY noted that “privately collected digital data could be a necessary requirement for policy making, governance and public service delivery in many areas.”<sup>92</sup> The Committee submitted its preliminary report in July 2020<sup>93</sup> and a revised draft was submitted on 16 December 2020.<sup>94</sup>

“Most of these laws have originated in the EU, as it is considered the vanguard of ensuring contestable and fair digital markets.”

The Kris Gopalakrishnan committee recommended that in the case of non-personal data, a particular ‘community’<sup>d</sup> can exercise its rights on High Value Datasets (HVDs).<sup>e,95</sup> An inclusive list is provided that mentions purposes for which sharing of non-personal data can be mandated as an HVD.

The Committee has recommended a responsibility/obligation for data custodians whenever requests are made for defined data-sharing purposes.<sup>96</sup>

<sup>d</sup> Defined by the committee as any group of people that are bound by common interests and purposes and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entirely virtual community.

<sup>e</sup> An HVD is a dataset that is beneficial to the community at large and shared as a public good.

# Pillars of a Sound Regulatory Framework

The committee declares HVD as a public good which can be shared for the benefit of the community or public goods, research and innovation, for policy development, and better delivery of public services.<sup>97</sup> It appears that not only a particular community but the government as well can ask for access to an HVD data set on these grounds.<sup>98</sup> Additionally, data can be requested for sovereign purposes.<sup>99</sup> Once again, the committee suggests a non-exhaustive list.

**Comment:** The Kris Gopalakrishnan Committee understands the economic and societal value of non-personal data. The mechanism that it employs, however, is by creating a mandatory data-sharing framework for the so-called HVD. The committee suggests that “India has rights over data of India, its people and organisations”<sup>100</sup> and treats this as a guiding principle towards its goal of “[establishing] rights of India and its communities over its non-personal data.”<sup>101</sup>

This mandatory data sharing may prove useful in the short run. In the long run, however, it may stifle innovation. A long-term approach to data sharing should be based on an incentive-based mechanism. As opposed to the mandatory non-personal data sharing recommended in India, the EU Data Governance Act proposes building trust to facilitate voluntary data sharing based on altruism.

Further, the scope of HVD is broad.<sup>102</sup> The Committee provides that a data trustee of HVD may levy a nominal charge to the Data Requesters.<sup>103</sup> However, it is not clear if this ‘nominal charge’ can be the ‘marginal cost’. It also appears problematic that the Committee considers an HVD dataset as a public good.<sup>104</sup> Non-rivalry and non-excludability are the two characteristics of a public good. It is doubtful that a particular data set always displays these characteristics.

The committee suggests that when data sharing involves access to private companies’ trade secrets or other proprietary information regarding their employees, or internal process and productivity data, such non-personal data will not be included for sharing.<sup>105</sup> This safeguard, however, is not sufficient as data collection itself includes investment and, at times, innovation. A broad mandate to share such data, therefore, may adversely affect business interest.

## 5.2 Use of Public Sector Data

### *Status: In force*

The public sector is one of the most data-intensive sectors.<sup>106</sup> This data can be reused to foster public welfare. For instance, health data with public bodies can be put to use by innovative private players in developing new medicines or modes of treatment.

The EU took steps in this direction and allowed for sharing of data held by public sector bodies through the 2003 Directive on Re-Use of Public Sector Information (PSI Directive).<sup>107</sup> The PSI Directive covered written texts, databases, audio files and film fragments. It does not apply, however, to the educational, scientific and broadcasting sectors. After its 2013 revision, content held by museums, libraries and archives also fell within the Directive's scope of application.<sup>108</sup> The PSI Directive has since been replaced by 'Open Data Directive'.<sup>109</sup>

Aside from the EU, other jurisdictions have instituted a framework for sharing public-sector data. In Canada, for instance, to facilitate government data sharing, the Open Government Portal was launched in 2014. Similarly, Mexico established its Open Data Initiative in 2015.<sup>110</sup>

In India, the National Data Sharing and Accessibility Policy (NDSAP) was introduced in March 2012 to make non-sensitive government data accessible online.<sup>111</sup> The MeitY, through the National Informatics Centre (NIC) has set up the Open Government Data (OGD) Platform India<sup>112</sup> to provide open access by the proactive release of the data available with various ministries, departments, and organisations of the Government of India. In February 2021, the Indian Government liberalised the geospatial data and geospatial data services including maps, and further allowed sharing of geospatial data produced using public funds, except the classified geospatial data collected by security and law enforcement agencies, for scientific, economic and developmental purposes to all Indian entities and without any restrictions on their use.<sup>113</sup>

**Comment:** The OGD platform has datasets that are incomplete and are rarely updated.<sup>114</sup> Also, some departments have stopped putting their data in the public domain.<sup>115</sup>

### 5.3 Business to Government (B2G) Data Sharing

#### *Status: In Process*

A reverse form of public sector data sharing is Business to Government (B2G) data sharing.<sup>116</sup> The private sector has access to data that can prove useful in guiding policy decisions or improve public services and thus sharing this data can further the public interest.<sup>117</sup> For instance, private sector data can lead to a more targeted response to epidemics, better urban planning, improved road safety and traffic management, as well as better environmental protection, market monitoring and consumer protection. The government can get faster insights on population movements, prices, inflation, the internet economy, energy or traffic.<sup>118</sup>

As discussed earlier, in the EU, the proposed Data Governance Act aims at sharing of business data with the government on altruistic grounds.

**Comment:** In India, the NPD framework suggested by the Kris Gopalakrishnan committee opts for a mandatory business data sharing. Businesses may be mandated to share their data to further public interest or for sovereign purposes. As shown above, these exceptions are couched in broad terms and could adversely affect business.


“India has a National Data Sharing and Accessibility Policy that allows for non-sensitive government data to be made accessible online.”

# Conclusion

**Vikas Kathuria** is Fellow at ORF, and Affiliated Researcher at Max Planck Institute for Innovation and Competition, Munich.

**D**igital markets in India are rapidly growing. In view of the importance of these markets, the paper took an exploratory study of laws and regulations that can ensure their fairness and contestability. These twin objectives, in turn, can ensure consumer welfare. The paper analysed the following laws that together set out this framework that may act as a toolkit for a fair and contestable digital market: (i) competition law, (ii) ex-ante regulation for digital ‘gatekeepers’, (iii) laws for increased transparency in Platform to Business (P2B) transactions, (iv) law on personal data protection, and (v) laws on governing access and sharing of data.

The paper discussed international precedents in the above areas of law and regulations, discussed the Indian legal landscape (also regulatory) on each such area, and provided a brief critique. As most jurisdictions are still struggling to understand the complexities involved in digital markets, there are not many international precedents. The EU, however, has moved swiftly to ensure accountability and welfare in digital markets. Thus, the paper discussed the EU precedents and explored the Indian legal framework on these laws. While some such laws have been adopted in India (e.g. competition law and laws governing public sector data access), other areas are under deliberation (e.g. personal data protection, personal and non-personal data sharing). Importantly, certain laws have escaped the policy debate altogether (e.g. ex-ante regulation for powerful digital firms to complement competition law and P2B regulations). The paper advocates adoption of this toolkit after a proper contextualisation against the socio-economic backdrop of India.

To be sure, the draft National E-commerce Policy in India addresses issues pertaining to consumer protection, data privacy, and maintenance of a level playing field in the e-commerce sector.<sup>119</sup> The government may also consider creating a regulator for e-commerce.<sup>120</sup> In view of the importance of the growing e-commerce sector such steps are laudable. If, however, the suggested framework in this paper is adopted, it will benefit the overall digital markets in India. 

**Table 2:  
Regulatory Elements: A Snapshot**

Law/ Regulation	Purpose	Status	Comments
1. Competition Law	To protect and promote competition in digital markets	Present	<ol style="list-style-type: none"> <li>India has faced similar challenges that more mature jurisdictions have face in the digital economy.</li> <li>CCI acknowledges that digital markets are unique and require swifter intervention.</li> </ol>
2. Ex-ante regulation for digital 'gatekeepers'	Complement competition law in protecting and promoting competition in digital markets	Absent	<ol style="list-style-type: none"> <li>Germany has already adopted a set of ex ante regulation, while the EU and even China are in the process of adoption. India, being a crucial digital market, cannot stay behind.</li> </ol>
3. Regulations for Increased Transparency in Business to Business (B2B) transactions	Ensures transparency and trust in Platform-to-Business (P2B) transactions	Absent	<ol style="list-style-type: none"> <li>In its E-Commerce Market Enquiry Report, the CCI found several unfair practices in Platform-to-Business (P2B) Conduct.</li> <li>Self-regulation proposed by the CCI may not be suitable in view of the market power and information symmetry in this sector.</li> <li>The EU P2B Regulations can provide guidance.</li> </ol>

# Conclusion

<p>4. Laws on Personal Data Protection</p>	<p>To ensure users' privacy and security, and create trust in the digital economy</p>	<p>In Process</p>	<ol style="list-style-type: none"> <li>1. The draft Data Protection Bill, 2019, proposes wide exceptions for the Central Government.</li> <li>2. Limited checks have been imposed on state surveillance.</li> <li>3. The structure of the Data Protection Authority has also been criticized.</li> <li>4. It may also increase compliance cost.</li> </ol>
<p>5. Laws on governing Access and Sharing of data.</p>	<p>Unlock the societal and economic benefits of data sharing</p>		
<p><i>5.1 Non-personal data sharing in India</i></p>		<p>In Process</p>	<ol style="list-style-type: none"> <li>1. Instead of creating an incentive-based (or voluntary) data sharing framework, the draft NPD Protection Bill mandates data sharing for community and sovereign purposes. This may be counterproductive in the long run.</li> </ol>
<p><i>5.2 Use of Public Sector Data</i></p>		<p>Present</p>	<ol style="list-style-type: none"> <li>1. Some OGD have datasets that are incomplete and rarely updated.</li> <li>2. Some departments have stopped putting their data in the public domain.</li> </ol>

# Conclusion

<p>5.3 <i>Business to Government (B2G) Data Sharing</i></p>		<p>In Process</p>	<p>1. Mandating businesses to share their data to further public interest or for sovereign purposes, may be counterproductive.</p>
---	--	-------------------	--

*(Author's note: I am grateful to Sabrina Korreck and Arjun Jayakumar for helpful comments on an earlier draft of this paper. Thanks are also due to an anonymous reviewer. All errors are my own.)*



- 1 Statista, “India: Estimated total population from 2015 to 2025”, <https://www.statista.com/statistics/263766/total-population-of-india/>
- 2 Abhijit Ahaskar, “India pips US to become second-largest smartphone market after China in 2019”, Mint, February 07, 2020, <https://www.livemint.com/technology/gadgets/india-pips-us-to-become-second-largest-smartphone-market-after-china-in-2019-11581071893368.html>
- 3 IBEF, “Digital India: Power to Empower”, <https://www.ibef.org/blogs/digital-india-power-to-empower>
- 4 BDO United States, “COVID-19 is accelerating the rise of the digital economy”, <https://www.bdo.com/insights/business-financial-advisory/strategy,-technology-transformation/covid-19-is-accelerating-the-rise-of-the-digital-e>
- 5 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, “Competition Policy for the Digital Era” (2019) European Commission, <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>; Jason Furman et al, “Unlocking digital competition: Report of the Digital Competition Expert Panel”, (March 2019) © Crown Copyright 2019, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/785547/unlocking\\_digital\\_competition\\_furman\\_review\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf)
- 6 The proposed toolkit, therefore, comprises of both laws and regulations.
- 7 For a brief introduction of intermediary liability in India see, Saumya Kapoor, “Tracing the development of “intermediary liability” in India”, Lexology, <https://www.lexology.com/library/detail.aspx?g=be8df572-55b1-499a-85cf-8b44b59ee0bc#:~:text=Thus%2C%20intermediary%20liability%2C%20which%20is,the%20user%20on%20their%20platform.&text=Thus%2C%20there%20is%20a%20need,greater%20liability%20on%20the%20intermediaries>.
- 8 For a background of cybersecurity laws in India see, Aprajita Rana and Rohan Bagai, “Cybersecurity in India”, Lexology, <https://www.lexology.com/library/detail.aspx?g=4cd0bdb1-da7d-4a04-bd9c-30881dd3eadf#:~:text=India%20does%20not%20have%20a,and%20the%20cybercrimes%20associated%20therewith>.
- 9 For details see, CCI, “Introduction to Competition Law: (Part 1- Basic Introduction)”, [https://www.cci.gov.in/sites/default/files/advocacy\\_booklet\\_document/CCI%20Basic%20Introduction\\_0.pdf](https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/CCI%20Basic%20Introduction_0.pdf)
- 10 The Competition Act, 2002, [https://www.cci.gov.in/sites/default/files/advocacy\\_booklet\\_document/The%20Competition%20Act%2C%202002%20No.%2012%20of%202003.pdf](https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/The%20Competition%20Act%2C%202002%20No.%2012%20of%202003.pdf)
- 11 CCI, “About CCI”, <https://www.cci.gov.in/about-cci>
- 12 Adam Satariano, “Facebook Loses Antitrust Decision in Germany Over Data Collection”, The New York Times, June 23, 2020, <https://www.nytimes.com/2020/06/23/technology/facebook-antitrust-germany.html>
- 13 See, European Commission, Google Search (Shopping) Google (Shopping) , [https://ec.europa.eu/competition/elojade/isef/case\\_details.cfm?proc\\_code=1\\_39740](https://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740); European

- Commission, Antitrust: Commission fines Google ₹4.34 billion for abuse of dominance regarding Android devices, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_18\\_4581](https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581).
- 14 European Commission, Antitrust: Amazon, [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2077](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077)
  - 15 European Commission, Antitrust: Commission opens investigations into Apple, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_1073](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1073)
  - 16 Steven Pearlstein, “Facebook and Google cases are our last chance to save the economy from monopolization”, The Washington Post, December 18, 2020, <https://www.washingtonpost.com/business/2020/12/18/google-facebook-antitrust-lawsuit/>
  - 17 CCI, Case No. 01 of 2020, Rubtub Solutions Pvt. Ltd. V MakeMyTrip India Pvt. Ltd. (MMT), <https://www.cci.gov.in/sites/default/files/01-of-2020.pdf>
  - 18 CCI, Case No. 15 of 2020, Harshita Chawla v WhatsApp Inc, <https://www.cci.gov.in/sites/default/files/15-of-2020.pdf>
  - 19 CCI, Case No. 40 of 2019, Delhi Vyapar Mahasangh v Flipkart Internet Private Limited and its affiliated entities and Amazon Seller Services Private Limited and its affiliated entities, <https://www.cci.gov.in/sites/default/files/40-of-2019.pdf>
  - 20 CCI, Cases Nos. 7 and 30 of 2012, Matrimony.com Limited v. Google, 8 February 2018, <http://www.cci.gov.in/sites/default/files/07%20%26%20%2030%20of%202012.pdf>.
  - 21 CCI, Case No. 39 of 2018, Mr. Umar Javeed et al v Google, <https://www.cci.gov.in/sites/default/files/39-of-2018.pdf>
  - 22 CCI, Case No. 07 of 2020, XYZ v Google, <https://www.cci.gov.in/sites/default/files/07-of-2020.pdf>
  - 23 CCI, Market Study on E-Commerce in India: Key Findings and Observations 08-01-2020, [https://www.cci.gov.in/sites/default/files/whats\\_newdocument/Market-study-on-e-Commerce-in-India.pdf](https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf)
  - 24 Mr. Ashok Kumar Gupta, “Regulating the Digital Economy”, U.S.-India Business Council, Virtual Roundtable Keynote Address, July 29, 2020, <https://www.cci.gov.in/sites/default/files/speeches/USIBC.pdf?download=1>
  - 25 Mr. Ashok Kumar Gupta, “Regulating the Digital Economy”.
  - 26 See Furman et al. Note 10 above; Crémer et al. Note 10 above; Stigler Committee on Digital Platforms, Final Report, September 2019, <https://research.chicagobooth.edu/stigler/media/news/committee-on-digitalplatforms-final-report>
  - 27 Maria Lancieri, Filippo and da Silva Pereira Neto, Caio Mario, Designing Remedies for Digital Markets: The Interplay Between Antitrust and Regulation (February 17, 2021). FGV Direito SP Research Paper Series, SSRN: <https://ssrn.com/abstract=3704763> or <http://dx.doi.org/10.2139/ssrn.3704763>

- 28 Vikas Kathuria, “Ex-ante regulation for digital markets in India”, ORF, <https://www.orfonline.org/expert-speak/ex-ante-regulation-digital-markets-india/#:~:text=While%20the%20CCI%20is%20doing,of%20regulation%20is%20already%20felt.&text=Consequently%2C%20India%20should%20adopt%20binding,ups%20and%20fairness%20for%20users.>
- 29 See Note 30 above.
- 30 Proposal for a Regulation of the European Parliament and of The Council on contestable and fair markets in the digital sector (Digital Markets Act), Brussels, 15.12.2020 COM (2020) 842 final.
- 31 See in general, Jonathan B. Baker & Fiona Scott Morton, “Antitrust Enforcement Against Platform MFNs” (2018) 127 (7) *The Yale Law Journal* 2176-2202.
- 32 See Note 27 above.
- 33 [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_2077](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077)
- 34 For an unofficial English translation, see <https://www.d-kart.de/wp-content/uploads/2021/01/GWB-2021-01-14-engl.pdf>
- 35 Sec 19 (a) (2) GWB.
- 36 James Marshall and Thomas Reilly, “UK CMA Published Recommendations for the Regulation of Digital Markets”, *The Covington View*, <https://www.covcompetition.com/2020/12/uk-cma-published-recommendations-for-the-regulation-of-digital-markets/>
- 37 “China issues new anti-monopoly rules targeting its tech giants”, February 7, 2021, <https://www.cnbc.com/2021/02/07/china-issues-new-anti-monopoly-rules-targeting-its-tech-giants.html>
- 38 Competition & Market Authority, UK, “Online platforms and digital advertising: Market study final report”, July 1, 2020, [https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final\\_report\\_1\\_July\\_2020\\_.pdf](https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf)
- 39 EU Science Hub, “The EU Digital Markets Act”, <https://ec.europa.eu/jrc/en/publication/eu-digital-markets-act>
- 40 Recital 2. Regulation (EU) 2019/1150 of The European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
- 41 Christoph Busch, “The P2B Regulation (EU) 2019/1150: Towards a “procedural turn” in EU platform regulation?” (2020), 9, *Journal of European Consumer and Market Law*, Issue 4, pp. 133-134, <https://kluwerlawonline.com/journalarticle/Journal+of+European+Consumer+and+Market+Law/9.4/EuCML2020055>
- 42 Recital 3. Regulation (EU) 2019/1150, see Note 48 above.
- 43 Article 5 (1), Regulation (EU) 2019/1150.

- 44 Article 5(2), Regulation (EU) 2019/1150.
- 45 Article 10 (1), Regulation (EU) 2019/1150.
- 46 Vikas Kathuria, “The Antitrust App Store Wars Come to India “, SpicyIP, November 22, 2020, <https://spicyip.com/2020/11/the-antitrust-app-store-wars-come-to-india.html>
- 47 CCI, Market Study on E-Commerce in India, see Note 32 above, page 5.
- 48 CCI, Market Study on E-Commerce in India.
- 49 CCI, Market Study on E-Commerce in India, page 20
- 50 CCI, Market Study on E-Commerce in India, page 21
- 51 CCI, Market Study on E-Commerce in India, page 22
- 52 CCI, Market Study on E-Commerce in India, page 23.
- 53 CCI, Market Study on E-Commerce in India, page 24.
- 54 CCI, Market Study on E-Commerce in India, page 24.
- 55 CCI, Market Study on E-Commerce in India, page 25.
- 56 Through a ‘narrow’ parity clause an Online Travel Agent (OTA) strikes rate parity with respect to the rooms that a hotel lists on its own direct distribution channel. Thus, a room, which is also listed on the Online Travel Agent (OTA) portal, will always be equal or higher on the hotel’s own website. A ‘wide’ parity clause, additionally obtains rate parity vis-à-vis other competing portals.
- 57 CCI, Market Study on E-Commerce in India, see Note 32 above, pages 25-26.
- 58 The Bundeskartellamt, “Amazon removes price parity obligation for retailers on its Marketplace platform, B6-46/12”, 9 December 2013, [http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Kartellverbot/2013/B6-46-12.pdf%3F\\_\\_blob%3DpublicationFile%26v%3D2](http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Kartellverbot/2013/B6-46-12.pdf%3F__blob%3DpublicationFile%26v%3D2); The UK OFT also had opened investigation into wide MFN clauses adopted by Amazon, which was closed following Amazon’s decision to end this practice, <https://www.gov.uk/cma-cases/amazon-online-retailer-investigation-into-anti-competitive-practices>>; The Bundeskartellamt, Online hotel portal HRS’s ‘best price’ clause violates competition law – Proceedings also initiated against other hotel portals, [https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2013/20\\_12\\_2013\\_HRS.html](https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2013/20_12_2013_HRS.html) (affirmed by the Dusseldorf Higher Regional Court); see also, a joint investigation report by France, Italy, and Sweden, where Booking.com committed to change ‘wide’ parity clauses into ‘narrow’ parity clauses, Report On The Monitoring Exercise Carried Out In The Online Hotel Booking Sector by EU Competition Authorities in 2016, [https://ec.europa.eu/competition/ecn/hotel\\_monitoring\\_report\\_en.pdf](https://ec.europa.eu/competition/ecn/hotel_monitoring_report_en.pdf)
- 59 CCI, Market Study on E-Commerce in India, see Note 28 above, pages 25-27.
- 60 CCI, Market Study on E-Commerce in India, pages 25-27

- 61 GDPR.EU, “What is GDPR, the EU’s new data protection law?”, <https://gdpr.eu/what-is-gdpr/>
- 62 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).
- 63 “What is GDPR, the EU’s new data protection law?”, see Note 69 above.
- 64 “What is GDPR, the EU’s new data protection law?”
- 65 “What is GDPR, the EU’s new data protection law?”
- 66 Puttaswamy, 2017 (10) SCALE 1
- 67 MEITY, “Committee of Experts under the Chairmanship of Justice B.N. Srikrishna” (Srikrishna Committee Report), [https://www.meity.gov.in/writereaddata/files/Data\\_Protection\\_Committee\\_Report.pdf](https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf)
- 68 Srikrishna Committee Report, page 6.
- 69 Puttaswamy, see Note 70 above.
- 70 The Personal Data Protection (PDP) Bill, 2019, [http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373\\_2019\\_LS\\_Eng.pdf](http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf)
- 71 Anurag Vaishnav, “The Personal Data Protection Bill, 2019: All you need to know”, The PRS Blog, December 23, 2019, <https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know>
- 72 Aditi Agrawal, “A lowdown on Personal Data Protection Bill 2019”, Forbes India, Jan 28, 2021, <https://www.forbesindia.com/article/special/a-lowdown-on-personal-data-protection-bill-2019/66037/1>
- 73 Aditi Aggarwal, Forbes India.
- 74 PDP Bill, Chapter IV.
- 75 PDP Bill, Chapter V.
- 76 PDP Bill, Chapter X, Section 57 et seq.
- 77 PDP Bill, Sec 82 (1) (b)
- 78 PDP Bill, Sec 64.
- 79 Rishab Bailey, “The issues around data localisation”, The Hindu, February 25, 2020, <https://www.thehindu.com/opinion/op-ed/the-issues-around-data-localisation/article30906488.ece>; see also, Aditi Aggarwal, Forbes India, Note 80 above.
- 80 ORF, “The personal data protection bill 2019: Recommendations to the Joint

- Parliamentary Committee”, March 04, 2020, [https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/#\\_edn7](https://www.orfonline.org/research/the-personal-data-protection-bill-2019-61915/#_edn7).
- 81 Harshit Rakheja, “From Blanket Exemptions to Rising Cost of Compliance: The Personal Data Protection Bill Conundrum”, Inc42, February 11, 2021, <https://inc42.com/buzz/from-blanket-exemptions-to-rising-cost-of-compliance-the-personal-data-protection-bill-conundrum/>
- 82 European Commission, “A European Strategy for Data”, <https://ec.europa.eu/digital-single-market/en/european-strategy-data>
- 83 The OECD, “Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies”, <https://www.oecd.org/publications/enhancing-access-to-and-sharing-of-data-276aaca8-en.htm>, page 16.
- 84 The OECD, Enhancing Access to and Sharing of Data, page 11.
- 85 The OECD, Enhancing Access to and Sharing of Data, page 12.
- 86 The OECD, “Economic and social benefits of data access and sharing”, <https://www.oecd-ilibrary.org/sites/90ebc73d-en/index.html?itemId=/content/component/90ebc73d-en>
- 87 Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).
- 88 DIRECTIVE (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (Open Data Directive).
- 89 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information OJ L 345, 31.12.2003, p. 90–96
- 90 Recital 35, Proposed Data Governance Act, see Note 91 above.
- 91 Art 2(10), Proposed Data Governance Act.
- 92 GoI, MEITY, 13.09.2019, Constitution of a Committee of Experts to deliberate on Data Governance Framework, [https://www.meity.gov.in/writereaddata/files/constitution\\_of\\_committee\\_of\\_experts\\_to\\_deliberate\\_on\\_data\\_governance-framework.pdf](https://www.meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance-framework.pdf)
- 93 MEITY, Report by the Committee of Experts on Non-Personal Data Governance Framework, <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>
- 94 MEITY, Report by the Committee of Experts on Non-Personal Data Governance Framework, [https://static.mygov.in/rest/s3fs-public/mygov\\_160922880751553221.pdf](https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf), (Kris Gopalakrishnan committee report).
- 95 Kris Gopalakrishnan Committee Report, paragraph 7.6.
- 96 Kris Gopalakrishnan Committee Report, paragraph 7.4 (iii).
- 97 Kris Gopalakrishnan Committee Report, paragraph 8.2.

- 98 Kris Gopalakrishnan Committee Report, paragraph 8.2 (ii)
- 99 Kris Gopalakrishnan Committee Report, paragraph 8.1.
- 100 Kris Gopalakrishnan Committee Report, paragraph 3.4 (i)
- 101 Kris Gopalakrishnan Committee Report, paragraph 3.5 (i).
- 102 Kris Gopalakrishnan Committee Report, paragraph 7.6.
- 103 Kris Gopalakrishnan Committee Report, paragraph 7.7 (iv).
- 104 Kris Gopalakrishnan Committee Report, paragraph 7.8 (i).
- 105 Kris Gopalakrishnan Committee Report, paragraph 8.6.
- 106 European Commission, “From the Public Sector Information (PSI) Directive to the open data Directive”, March 10, 2021, <https://ec.europa.eu/digital-single-market/en/public-sector-information-psi-directive-open-data-directive>.
- 107 Directive 2003/98/EC of The European Parliament and of The Council of 17 November 2003 on the re-use of public sector information.
- 108 The OECD, “Policy initiatives enhancing data access and sharing”, <https://www.oecd-ilibrary.org/sites/baf19328-en/index.html?itemId=/content/component/baf19328-en>.
- 109 Directive (EU) 2019/1024 of the European parliament and of the council of 20 June 2019 on open data and the re-use of public sector information, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1024&from=EN>
- 110 The OECD, see Note 112 above.
- 111 MeitY, “National Data Sharing and Accessibility Policy (NDSAP)”, <https://dst.gov.in/national-data-sharing-and-accessibility-policy-0>; The Gazette of India, March 17, 2012, National Data Sharing and Accessibility Policy (NDSAP), <https://data.gov.in/sites/default/files/NDSAP.pdf>
- 112 Open Government Data (OGD) Platform India, <https://data.gov.in/>
- 113 Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services including Maps, February 15, 2021, <https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf>
- 114 Thejesh G N, “Open Data in India: In a Restrictive Copyright Regime, Voluntary Organisations Pitch in to Make Data Accessible” ISSN (Online) - 2349-8846, Economic & Political Weekly.
- 115 Thejesh G N, Economic & Political Weekly.
- 116 European Commission, “Experts say privately held data available in the European Union should be used better and more”, February 19, 2020, <https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more>

# Endnotes

- 117 European Commission, “FAQs on business-to-government data sharing”, <https://ec.europa.eu/digital-single-market/en/faq/faqs-business-government-data-sharing#:~:text=Key%20areas%20in%20which%20B2G,of%20ethical%20artificial%20intelligence%20services%2C>.
- 118 European Commission, “Guidance on private sector data sharing”, March 01, 2021, <https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing>.
- 119 DIPP, Draft National e-Commerce Policy, [https://dipp.gov.in/sites/default/files/DraftNational\\_e-commerce\\_Policy\\_23February2019.pdf](https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf).
- 120 “DPIIT ‘definitely’ working on new e-commerce policy: Govt official”, Business Standard, February 5, 2021, [https://www.business-standard.com/article/economy-policy/dpiit-definitely-working-on-new-e-commerce-policy-govt-official-121020500854\\_1.html#:~:text=The%20government%20in%202019%20had,locally%20and%20storing%20it%20abroad](https://www.business-standard.com/article/economy-policy/dpiit-definitely-working-on-new-e-commerce-policy-govt-official-121020500854_1.html#:~:text=The%20government%20in%202019%20had,locally%20and%20storing%20it%20abroad).

*Images used in this paper are from Getty Images/Busà Photography (cover and page 2) and Getty Images/Otto Stadler (back page)*



# Endnotes



**Ideas . Forums . Leadership . Impact**

20, Rouse Avenue Institutional Area,  
New Delhi - 110 002, INDIA  
Ph. : +91-11-35332000. Fax : +91-11-35332005  
E-mail: [contactus@orfonline.org](mailto:contactus@orfonline.org)  
Website: [www.orfonline.org](http://www.orfonline.org)