IDFC Institute's response to proposed amendments to the Consumer Protection (E-Commerce) Rules, 2020

Overview

IDFC Institute appreciates the opportunity to submit feedback on the amendments to the Department of Consumer Affairs's *Consumer Protection (E-commerce) Rules* (hereafter referred to as CPR). Based on our published research and experience in supporting government policy and implementation initiatives at both the Central and state levels, we are pleased to share our recommendations on the proposed amendments.

Context

India has the fastest growing e-commerce sector globally; it is projected to reach $200 billion in 2026 from $38.5 billion in 2017[1]. Much of this growth has been driven by a broadening of the market on both the demand and supply sides. A significant portion of the demand growth has come from Tier 2 and Tier 3 cities, while intermediary platforms have allowed micro, small and medium industries (MSMEs) and start-ups to reach these expanding markets with minimal capital outlay.

The consolidation of the e-commerce sector with a small number of entities such as Amazon, Flipkart and Paytm Mall entrenching and expanding their market shares -- through a series of mergers and acquisitions, partnerships and entry into adjacent e-commerce segments -- is the flipside of this. This comes at a time when digital retail models are rapidly becoming essential means of accessing markets for both buyers and sellers. The role that e-commerce has played during the COVID-19 pandemic -- order volume grew by 36% in the last quarter of 2020 despite the pandemic-exacerbated demand slump[2] -- underscores this.

A regulatory framework, therefore, must carefully balance the gains from e-commerce's efficiency and the need to protect consumers and prevent market distortions. We outline the specific principles that should serve as the foundation of such a framework.

1. Proportionality in regulation

A calibrated and differentiated approach towards regulating e-commerce entities, flowing from clarity about the entities to be regulated and the reasons for doing so, is essential given the vastly different costs and benefits for different actors.

To be fit for purpose, compliance measures must take into account business models, company size and e-commerce segment. A 'one size fits all' approach is liable to impose an unsustainable

[1] E-commerce in India: Industry Overview, Market Size & Growth| IBEF
[2] *Ibid.*

regulatory burden on many e-commerce entities, be counterproductive in terms of encouraging investment, innovation and job creation, and, in the long run, harm consumers. The attempts at differentiated regulation by other jurisdictions such as the European Union and US are useful references.

2. Transparency and Accountability

The rules underpinning regulation should ensure more transparency for consumers with respect to how entities operate their businesses and sell their goods or services and ensure there is a clear mechanism for recourse in case of violation of these principles. Given the nature of e-commerce entities, this would not only be with respect to transactions of goods and services, but how such entities collect, analyse and share data of users.

3. Regulatory Clarity

Regulatory clarity is essential -- both for clearly demarcating the jurisdictions of different regulatory authorities and for synchronising the e-commerce regulatory framework with other relevant regulations. Regulatory overlaps where multiple agencies have oversight over similar activities could lead to unnecessary costs for both the entities regulated as well as the agencies themselves. And contradictory policies and regulations will increase market uncertainty, make effective implementation impossible and lead to turf battles between different authorities.

Thematic comments and recommendations

We have divided our specific comments on the amendments to the e-commerce rules into four categories which include:

1. Need for a differentiated regulatory approach
2. Business practices
3. Consumer data protection
4. Regulatory overlap

1. Differentiated regulatory approach

a. Definition of e-commerce entities

Section 3(*b*) *"e-commerce entity" means any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, including any entity engaged by such person for the purpose of fulfilment of orders placed by a user on its platform and any 'related party' as defined under Section 2(76) of the Companies Act, 2013, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity*

This definition has an extremely broad scope. In terms of size, it includes both market leaders and small start-ups, and imposes the same regulatory burden on both. In terms of business model, it makes no distinction between intermediary platforms such as digital retail marketplaces, which are far more likely to play structurally crucial roles in the e-commerce sector, and inventory-based digital storefronts. And in terms of e-commerce segments, it fails to account for the crucial different categories such as goods, online travel bookings and food tech that the Competition Commission of India's (CCI) 2020 *Market Study on E-commerce in India*[3] study threw up. It therefore lacks clarity about its purpose.

This is counterproductive. In addition to Amazon and Flipkart, India's e-commerce industry has a considerable number of small companies that account for nearly 40% of the market. According to the CCI report, 45% of manufacturing output comes from MSMEs and nearly 43% participate in online sales.[4] A 'one size fits all' approach will impose a disproportionate burden on smaller companies. This will have an upstream effect as well as affected e-commerce entities pass regulatory costs on to business users. In the medium-to-long term, this will harm both market contestability and consumers.

We suggest that the rules take into account the different categories of e-commerce entities and define and tailor the regulatory framework accordingly. Various jurisdictions have adopted such an approach. The European Union's Digital Markets Act (DMA) focuses on 'gatekeeper platforms' designated according to well-defined criteria and assessed periodically. The DMA uses quantitative metrics (annual turnover, number of users) in addition to qualitative metrics such as the platform serving as an "important gateway for business users to reach end users"[5] to classify large e-commerce entities and apply a differentiated regulatory policy.

In the UK, the newly-launched Digital Markets Unit which sits within the Competition and Markets Authority, will likewise have the power to give tech firms that hold significant and entrenched market power 'Strategic Market Status'. This will compel the designated entities to follow specific codes of conduct. And the US Congress' House Judiciary Committee passed the Ending Platform Monopolies Act in June which also incorporates a differentiated approach. Article (5)(B)(i)–(iii) of Section 5 of the Act detail an approach similar to the DMA, describing a 'covered platform' on the basis of quantitative metrics such as user base, net annual sales and market capitalisation, and a qualitative assessment of its role as "a critical trading partner for the sale or provision of any product or service offered on or directly related to the online platform"[6].

To this end, we recommend that the CPR clearly delineate the e-commerce entities it applies to, or delineate differentiated obligations, on the basis of:

i. User base and other quantitative metrics that may be relevant

[3] Market Study of E-commerce in India
[4] *Ibid.*
[5] Digital Markets Act, 2020
[6] H.R.3825 - 117th Congress (2021-2022): Ending Platform Monopolies Act

ii. Whether or not the entity is an intermediary platform
iii. The e-commerce segment the entity operates in

b. Appointment of Chief Compliance Officer, nodal contact person and Resident Grievance Officer

Section 5.5(a) *appoint a Chief Compliance Officer who shall be responsible for ensuring compliance with the Act and rules made thereunder and shall be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that e-commerce entity where he fails to ensure that such entity observes due diligence while discharging its duties under the Act and rules made there under:*

Section 5.5(b) *appoint a nodal contact person for 24x7 coordination with law enforcement agencies and officers to ensure compliance to their orders or requisitions made in accordance with the provisions of law or rules made thereunder.*

Section 5.5(c) *appoint a "Resident Grievance Officer", who shall, subject to clause (b), be responsible for the functions referred to in sub-rule (2) of rule 3.*

Smaller entities with limited revenue and employee bases will face an undue burden in complying with these regulations. The need for them to have these personnel is unclear, besides; they will not face the same volume of complaints or law enforcement compliance directives as large platforms. This section also raises an enforcement dilemma. Ensuring that small entities comply consistently will be unfeasible. At the same time, the potential for punitive action against such entities that may be found to be in violation could have a chilling effect.

We therefore suggest that Sections 5.5.(a) - (c) be applicable only to e-commerce entities that merit the highest degree of scrutiny as per our previous recommendation.

c. Fall-back liability

Section 5.9 *A marketplace e-commerce entity shall be subject to a fall-back liability where a seller registered on its platform fails to deliver the goods or services ordered by a consumer due to negligent conduct, omission or commission of any act by such seller in fulfilling the duties and liabilities in the manner as prescribed by the marketplace e-commerce entity which causes loss to the consumer.*

A fall-back liability on marketplace e-commerce entities could create several unintended consequences:

i. It could disincentivise small e-marketplaces that are capital-poor and raise barriers to entry.

ii. It would create a moral hazard for sellers who would be absolved of liability for the product or service sold.
iii. As a counter to the previous problem, e-marketplaces could charge a commission per sale as 'insurance' or stipulate an amount be held in escrow. This would penalise all sellers instead of only those guilty of negligence or misconduct. It would also have a chilling effect on capital-poor sellers.

This provision that has no equivalent in other jurisdictions across the world. We recommend that it be removed.

2. Business practices

a. Country of origin

Section 5.7(b) *identify goods based on their country of origin, provide a filter mechanism on their e-commerce website and display notification regarding the origin of goods at the pre-purchase stage, at the time of goods being viewed for purchase, suggestions of alternatives to ensure a fair opportunity for domestic goods;*

We suggest removing this clause for the following reasons:
i. Ascertaining the country of origin of many goods will be difficult given the complex nature of global supply and value chains.
ii. This could become a contentious international trade issue as the WTO agreement on rules of origin[7] mandate that the member country's policy should clarify in detail the specifications/criteria for determining the country of origin, and not be used as an instrument to pursue trade objectives.
iii. Providing domestic alternatives to non-Indian goods is, by definition, distortionary, with a number of potential consequences such as disincentivising tie-ups between Indian e-marketplaces and foreign sellers.

b. Flash sales

Section 5.16 *No e-commerce entity shall organize a flash sale of goods or services offered on its platform.*

We suggest removing this section given the ambiguity over the definition of a conventional sale versus a flash sale. Flash sales as defined now with their deep discounts benefit consumers through offering lower prices. They can also benefit sellers by growing the customer base.

We recognise that dominant marketplace platforms may compel sellers to participate in such sales. This and the potential long-term consequences for consumers – "a risk to competition on

[7] Agreement on Rules of Origin

non-price aspects such as quality and innovation" as per the CCI report[8] -- qualify as abuse of dominance and consumer welfare loss, however. Both of these are competition issues. This is therefore best tackled as an *ex post* regulatory problem by the CCI which can deal with a case on its merits. *Ex ante* regulation under the CPR, on the other hand, would be too broad an approach, potentially harming consumers and sellers both.

3. Consumer data protection

a. Consent for data collection and sharing

Section 5.14(e) *[No e-commerce entity shall] make available any information pertaining to the consumer to any person other than the consumer without the express and affirmative consent of such consumer, no such entity shall record such consent automatically, including in the form of pre-ticked checkboxes*

Consumer data in the individual and the aggregate fuels e-commerce business models. There is therefore substantial incentive for e-commerce entities to use this data in a manner that benefits them but may run counter to the interests and wishes of consumers. While this clause attempts to address this problem, it faces two problems: it is redundant and it may entrench business users' lack of countervailing power vis-a-vis marketplace platforms.

Firstly, the IT Act, 2000 currently addresses breaches of confidentiality and privacy. Evolving legislation will do so far more exhaustively. The draft Personal Data Protection Bill, 2019 lays out significant responsibilities for data fiduciaries. Any future non-personal data regulatory framework may also be pertinent for aggregated and anonymised customer data. Section 5(14)(e), therefore, is unnecessary. Further, by mandating a far more limited privacy protection mandate for e-commerce entities than evolving legislation, it will create regulatory uncertainty that is liable to leave consumers more vulnerable.

Secondly, market research has shown that business users lack bargaining power in relation to dominant e-commerce platforms. This is due at least partly to the latter's control of data pertaining to consumers[9]. While consumers' control of their data must remain paramount, Section 5.14(e)'s attempt to do this via e-commerce platforms is likely to result in negative competition outcomes and a decrease in consumer welfare.

We recommend that this section be amended to:

- Mandate that e-commerce entities follow the rules, guidelines and standards established by enumerated, relevant laws for dealing with consumer data
- Mandate that marketplace e-commerce entities establish mechanisms that allow business users to request consumer data in an equivalent manner, undertaking similar obligations

[8] Market Study of E-commerce in India
[9] *Ibid.*

and liabilities vis-a-vis consumer data. The European Union's Digital Markets Act provides an example of this. Please see below for the relevant clause.

- Digital Markets Act, Section 11(2): "*Where consent for collecting and processing of personal data is required to ensure compliance with this Regulation, a gatekeeper shall take the necessary steps to either enable business users to directly obtain the required consent to their processing, where required under Regulation (EU) 2016/679 and Directive 2002/58/EC, or to comply with Union data protection and privacy rules and principles in other ways including by providing business users with duly anonymised data where appropriate. The gatekeeper shall not make the obtaining of this consent by the business user more burdensome than for its own services.*"

Section 5.18 *Every e-commerce entity shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents*

This clause flows from Section 2(47)(j)(ix) of the Consumer Protection Act, 2019. This Section pertains to unfair trade practices that "for the purpose of promoting the sale, use or supply of any goods or for the provision of any service, adopts any unfair method or unfair or deceptive practice". It has no relevance for government access to e-commerce entities' data; the related clause in the CPR is therefore misplaced. In addition, 5(18) grants extensive powers to government bodies to demand data from e-commerce entities without judicial oversight, conditionalities and other checks and balances.

This runs counter to the principles of legality, proportionality, necessity (or legitimate goal) and procedural guarantees[10] established by the Puttaswamy case -- particularly in the absence of a fit-for-purpose data protection law with the Personal Data Protection Bill, 2019, still in draft stage.

We therefore recommend that Section 5(18) be removed from the CPR and government access to data take place instead under data protection legislation.

4. Regulatory overlap

Section 5.17 *No e-commerce entity which holds a dominant position in any market shall be allowed to abuse its position.*

This section speaks to the CCI's domain. This could lead to confusion regarding the jurisdiction of different regulatory authorities. In the past, regulatory turf issues have led to unnecessary

[10] Proportionality Test for Aadhaar: The Supreme Court's two approaches

delays with respect to enforcement of the law. This has happened, for instance, between the Securities and Exchange Board of India and Insurance Regulatory and Development Authority of India on regulating Unit-Linked Investment Plans. CCI and the Telecom Regulatory Authority of India have also clashed over regulatory overlap.

As we have detailed in Section 3.a of this document, the CPR also has such regulatory confusion when it comes to personal data. This speaks to a larger issue. An e-commerce regulation must synergise with personal data protection, competition and any other relevant regulations. Its scope must be made clear keeping in mind the issues it wishes to address and the different purposes of *ex ante* regulation and *ex post* regulation such as most competition cases. We therefore recommend the following:

i. A section should be added delineating where and how the CPR intersects with other relevant legislations.
ii. Section 5.17 should be deleted.