RECONCILING 'FALL-BACK LIABILITY' AND 'SAFE HARBOUR' IN INDIA'S E-COMMERCE JURISPRUDENCE

Shraddha Seth, Guest Faculty at National Law University, Odisha and University Law College, Utkal University, Odisha

ABSTRACT

The exponential growth of India's e-commerce sector has created new forms of "social solidarity" but also new "social struggles," setting consumer protection against platform innovation, thereby resulting in a direct legislative conflict. The Consumer Protection Act (CPA), 2019, rooted in the jurisprudential shift to *caveat venditor*, proposes a "fall-back liability" clause, a form of "strict" or "secondary liability" based on risk. This contradicts the "safe harbour" immunity of Section 79 of the IT Act, 2000, which establishes a reactive, fault-based regime contingent on "actual knowledge".

This article analyzes this legal and doctrinal dichotomy. It examines the Indian judiciary's vacillating attempts to resolve the conflict, contrasting the "Objective Approach" (platform control) with the "Subjective Approach" (consumer perception) used by consumer forums and the statutory defense of safe harbour.

The paper evaluates the policy arguments, weighing the government's consumer-centric push against industry warnings of a "chilling effect" on economic innovation and growth. By drawing comparative lessons from the proactive diligence model of the EU's Digital Services Act (DSA), it proposes a harmonized "middle path. It concludes by proposing a harmonized regulatory framework, advocating for legislative amendments to incorporate 'Know Your Business Customer' (KYBC) norms into the IT Act's due diligence requirements and suggesting a tiered liability model for judicial application. This approach seeks to balance the imperative of consumer protection with the need to foster innovation and competition in India's burgeoning digital economy.

Introduction

As the legal theorist Duguit, influenced by Durkheim, pointed out, society is born from interdependence and thereby built on a "social solidarity". This solidarity arises because individual, unable to procure all necessities of life themselves, must rely on a complex "exchange of services" to meet their "diverse needs." As Duguit argued, law's fundalmental purpose is not to serve a higher principle but to serve the practical necessity of society's survival by securing and protecting this social solidarity.[1]

The Indian e-commerce market's meteoric rise is an example of this "social solidarity", transforming from a niche convenience into a cornerstone of the national economy. This digital revolution has created an unprecedented new form of interdependence, reshaping consumer behaviour and supply chains. However, this rapid expansion has also given rise to a new "social struggle", a concept Ihering noted as the very origin of law. The often anonymous and disintermediated nature of online marketplaces created significant information asymmetry, leaving consumers vulnerable to fraud , defective products and their claims going unresolved effectively.

At the heart of this evolving landscape lies the law's attempt to harmonize the conflicting interests arising from this new struggle. This has created a profound legal and philosophical dichotomy, embodied by two powerful but conflicting statutes. The first is the Consumer Protection Act, 2019 (CPA 2019), a landmark legislation rooted in a philosophy of holding all participants accountable, thereby seeking to secure "social solidarity" for the consumer by upholding their rights and addressing their claims from violation of those rights. In direct opposition stands Section 79 of the Information Technology Act, 2000 (IT Act), which was enacted to nurture the growth of this new marketplace by granting a conditional 'safe harbour' immunity to the intermediary platforms that facilitate it.

This legislative conflict has reached a critical flashpoint with the proposed introduction of a "fall-back liability" clause in the draft amendments to the E-Commerce Rules 2020 (E-Commerce Rules). This provision, which seeks to make marketplace entities directly liable for the failures of third-party sellers, represents the most forceful assertion yet of the consumer

[1] Dr N.V Paranjape, Studies in Jurisprudence & Legal theory XXXX (9th ed. 2019) (1994).

protection paradigm[2]. It directly challenges the intermediary immunity granted by the IT Act, creating a state of legal ambiguity where e-commerce platforms find themselves at a crossroads- simultaneously defined as protected intermediaries under one law and potential guarantors under another.

This article aims to navigate this complex intersection of consumer rights and technology law. It will begin by tracing the doctrinal shift in Indian consumer law from caveat emptor to caveat venditor, which provides the philosophical foundation for the CPA 2019. It will then dissect the specific statutory mechanics of both the CPA 2019's liability regime and the IT Act's safe harbour provision. Subsequently, the article will analyse the judiciary's inconsistent attempts to resolve this tension through key precedents. By evaluating the competition policy arguments and drawing lessons from international regulatory model in the European Union, this article will conclude by proposing a harmonized framework designed to provide legal certainty, protect consumers, and sustain the innovative dynamism of India's e-commerce sector.

From *Caveat Emptor* to *Caveat Venditor:* The Philosophical Foundation

As Savigny an exponent of historical school of jurisprudence pointed out law grows with the growth of the society and gains its strenghth from the society, the legal framework established by the Consumer Protection Act, 2019, is not a sudden legislative development but the culmination of a gradual jurisprudential evolution in Indian commercial law. This marks a pragmatic shift from the 19th-century doctrine of *caveat emptor* ('let the buyer beware') to the principle of caveat venditor ('let the seller beware'). Analyzing this philosophical transition is essential to appreciating the legislative intent behind imposing stricter liabilities on all market participants, including e-commerce marketplaces.

The Traditional Regime Caveat Emptor

The doctrine of *caveat emptor* was a cornerstone of traditional contract and sale of goods law, inherited from British colonial jurisprudence and formally codified in India's Sale of Goods Act, 1930. This principle placed the onus of diligence, inspection, and risk squarely on the shoulders of the buyer. It operated on the assumption of a marketplace characterized by simple,

[2] Vidhi Madan, *'Fall-back liability' under the Consumer Protection (e-Commerce) Rules, 2020: Stricter norms in digital diaspora*, Lakshmikumaran & Sridharan: Top Law Firm in India (Oct. 19, 2021), https://www.lakshmisri.com/insights/articles/fall-back-liability-under-the-consumer-protection-e-commerce-rules-2020-stricter-norms-in-digital-diaspora/.

tangible goods and a relative symmetry of information and bargaining power, where a buyer could reasonably be expected to examine a product and use their own skill and judgment to assess its quality and fitness for purpose.[3]

The statutory embodiment of this doctrine is found in Section 16 of the Sale of Goods Act, 1930. This provision explicitly states that, under a contract of sale, subject to certain exceptions, there is no implied warranty or condition as to the quality or fitness for any particular purpose of goods supplied.[4] In essence, the law presumed that the buyer, having had the opportunity to inspect the goods, accepted them 'as is'. Unless the seller engaged in active fraud or provided an express warranty, the buyer had little to no recourse if the product later proved defective or unsuitable. This legal posture prioritized the finality of transactions and protected the seller from subsequent liability, reflecting a view that prioritized business interests over those of the consumer.

The Shift to Caveat Venditor

Over the latter half of the 20th century, the principle of *caveat emptor* began to change. This was not due to a change in legal theory, but as a direct response to the changing situation of the marketplace. The industrial revolution and the advent of mass production[5] led to increasingly complex goods, from electronics to pharmaceuticals, whose inner workings and potential defects were far beyond the inspection capabilities of an ordinary consumer. This created a significant information asymmetry, where manufacturers and sellers possessed vastly more knowledge about their products than buyers. The doctrine of *caveat emptor* became manifestly unfair in this new context, allowing sellers to exploit this information gap to the detriment of consumers.

Recognizing this imbalance, Indian jurisprudence and legislation began a slow but steady pivot towards *caveat venditor*. This principle shifts the burden of responsibility, requiring the seller to ensure that the products they sell are of a certain quality, fit for their intended purpose, and free from defects. It places an obligation on the seller to be transparent and accountable for the

[3] Sarrah Nayar, *THE SHIFTING PARADIGM: FROM CAVEAT EMPTOR TO CAVEAT VENDITOR*, 4 INDIAN J. LEGAL REV. 98, XXXX (2024), https://ijlr.iledu.in/wp-content/uploads/2024/06/V4I214.pdf.
[4] Id.
[5] Aishwarya Agrawal, *LawBhoomi*, lawbhoomi: Caveat Venditor (July 16, 2024), https://lawbhoomi.com/caveat-venditor/.

goods they bring to market.[6]

The first major legislative manifestation of this shift was the enactment of the Consumer Protection Act, 1986, hailed as a 'Magna Carta' for consumers, as it formally recognized a set of consumer rights and established a three-tier, quasi-judicial redressal mechanism (District, State, and National Commissions) to provide efficient, speedy, and effective justice. It moved beyond the narrow boundaries of contract law and created a legal sphere dedicated to protecting consumer interests against defective goods and services, and unfair trade practices.

The Consumer Protection Act, 2019, embraces the *caveat venditor* doctrine in an elaborative and comprehensive manner. It strengthens the rights and redressal mechanisms of the 1986 Act but also explicitly expands its scope to address the challenges of the digital age, including e-commerce and direct selling. This long historical trajectory, from the ethical trade codes of ancient Indian texts like the *Manu Smriti* and Kautilya's *Arthashastra*, through the fragmented regulations of the colonial era, to the modern consumer protection regime, demonstrates a consistent legal progression towards greater seller accountability.[7] The CPA 2019, and by extension the concept of 'fall-back liability', legislative logically intends to address this trend, applying the principle of seller accountability forcefully to the online marketplace, where the consumer is arguably at their most vulnerable due to the lack of physical inspection and the anonymity of sellers.

The CPA 2019 and the Imposition of 'Fall-Back Liability'

The Consumer Protection Act, 2019, represents a legislative overhaul designed to modernize India's consumer protection regime and equip it to handle the complexities of the digital economy. A central feature of this modernization is the creation of a specific legal architecture to govern e-commerce transactions and hold online platforms accountable. This is achieved through a combination of expanded statutory definitions, detailed subordinate legislation in the form of the E-commerce Rules, and the introduction of novel liability concepts.

[6] Dr Sachin Babruvan Mane, *Caveat Emptor Vs Caveat Venditor and Consumer Protection Act*, IX Aayushi Int'l Interdisc. Rsch. J. (AIIRJ) 81, XXXX (2022), https://dayanandlaw.org/wp-content/uploads/2023/01/Article-18.pdf.

[7] Arpit Nayak, *Consumer affairs in India | History, Rights, Laws, Awareness, & Redress | Britannica*, Encyclopedia Britannica (Mar. 3, 2025), https://www.britannica.com/topic/consumer-affairs-in-India.

Amended Statutory Definitions

The CPA 2019 meticulously broadens key definitions to ensure that online transactions and the entities that facilitate them fall squarely within its regulatory purview. This definitional expansion is the foundational step that enables the application of consumer protection principles to the digital marketplace.

The definition of a "consumer" under Section 2(7) of the CPA 2019, was updated to explicitly include transactions conducted "through electronic means or by teleshopping or direct selling or multi-level marketing"[8], ensuring that an individual purchasing a product from an online marketplace enjoys the same status and protections as a customer in a physical store. The Act introduces a formal definition for "e-commerce," under Section 2(16) describing it as "buying or selling of goods or services including digital products over digital or electronic network".[9]This broad definition is technology-neutral and future-proof, encompassing not only physical goods ordered online but also the growing market for digital products like software, e-books, and streaming services. Electronic Service Provider defined under Section 2(17**)** perhaps the most critical definition for establishing platform liability. It defines an "electronic service provider" as a person who provides technologies or processes to enable a product seller to engage in selling goods or services to a consumer, and explicitly "includes any online market place or online auction sites".[10] This language directly targets platforms like Amazon and Flipkart, clarifying that their role as technological facilitators brings them within the ambit of the Act. They can no longer easily claim to be mere passive conduits with no responsibility for the transactions they enable.

The Consumer Protection (E-commerce) Rules, 2020

Building on the foundation laid by the CPA 2019, the Central Government notified the Consumer Protection (E-commerce) Rules, 2020, which prescribe detailed obligations for e-commerce entities. These rules translate the broad principles of the Act into specific, actionable duties.

[8] CONSUMER PROTECTION ACT, 2019, Law No. NO. 35 2019, Aug. 9, 2019, XXXX (India), https://ncdrc.nic.in/bare_acts/CPA2019.pdf.
[9] Id.
[10] Id.

The Inventory e-commerce entity, that owns the inventory of goods or services and sells them directly to consumers. These entities are akin to traditional sellers and are directly liable for the products they sell, including ensuring adverstisements are consistent with the product's actual characterstics and bearing liability if they vouch for the authenticity of goods.[11]

Other is the marketplace e-commerce entity that provides information technology platform on a digital network to facilitate transactions between independent buyers and sellers. The rules impose significant baseline of duties on all e-commerce entities, such an establishing a grievance redressal mechanism with a named Grievance Officer, acknowledging complaints within 48 hours, and resolving them within one month. They are also prohibited from adopting unfair trade practices, such as manipulating prices or refusing to take back defective goods. Crucially, the Rules impose specific and active liabilities on marketplace entities, moving them beyond the role of passive conduits. These includes: the marketplaces must display seller's full name, address, and contact details of all sellers on their platform, enabling consumers to make informed decisions. They must require sellers to provide an undertaking that their product descriptions other content corresponds to the actual product and are accurate. Marketplaces must provide an explanation of the main parameters used to determine rankings. The Rules also impose duties on the seller themselves, such as not posting false reviews, and providing all necessary information and other requirements.[12]

Significantly, the Rules directly acknowledge the conflict with the IT Act. Rule 5 state that a marketplace entity seeking the safe harbour exemption under section 79 of the IT Act, 2000, must comply with the due diligence requirements of that Act. This provision statutorily links the consumer protection framework to the intermediary liability framework, setting the stage for the legal conflict.

The 'Fall-Back Liability' Clause

The most potent and controversial extension of this consumer-centric regime is the proposed 'fall-back liability' clause, introduced in the Draft Consumer Protection (E-commerce) Amendment Rules, 2021. This clause represents a deliberate policy decision to shift the ultimate risk of a failed transaction from the consumer to the platform. The draft rules define

[11] DR.MARIAPPAN GOVINDARAJAN, *CONSUMER PROTECTION (E-COMMERCE) RULES, 2020 – AN OVERVIEW | TaxTMI*, TaxTMI: TaxTMI (Sept. 20, 2020), https://www.taxtmi.com/article/detailed?id=9460.
[12] Id.

'fall-back liability' as "the liability of a marketplace e-commerce entity where a registered seller... fails to deliver the goods or services ordered by a consumer due to negligent conduct, omission, or commission of any act by such seller" that results in a loss to the consumer. This provision makes the platform vicariously liable for the failures of a third-party seller, transforming its role from a facilitator to a de facto guarantor of the transaction's fulfillment.[13]

The government's stated rationale for this provision is to plug a critical gap in the consumer redressal framework. Policymakers and consumer groups observed that e-commerce platforms frequently evade responsibility for seller defaults by invoking their intermediary status under the IT Act, leaving consumers with little effective recourse against a distant, anonymous, or fraudulent seller.[14]The Parliamentary Standing Committee on Commerce explicitly rejected the platforms' argument that they have no control over the goods sold, placing the onus on them to act as a responsible intermediary in resolving complaints.[15] 'Fall-back liability' is the legislative tool designed to enforce this responsibility, ensuring that the consumer has a clear and accessible entity, the platform with which they have a direct relationship, to hold accountable. This clause is a forceful attempt to legislatively overrule the intermediary defense in the specific context of consumer e-commerce, prioritizing the consumer's right to a secure transaction above the platform's claim to neutrality.

Section 79[16] of the IT Act, 2000: The Shield?

Standing in contrast to the consumer-centric liability model of the CPA 2019 is the protective framework of Section 79 of the Information Technology Act, 2000. This provision, introduced through the IT (Amendment) Act, 2008, was designed to provide a 'safe harbour' for internet intermediaries, shielding them from liability for third-party content. Its primary legislative purpose was to foster the growth of India's digital economy by providing legal certainty to a

[13] Vidhi Madan, *'Fall-back liability' under the Consumer Protection (e-Commerce) Rules, 2020: Stricter norms in digital diaspora*, Lakshmikumaran & Sridharan: Top Law Firm in India (Oct. 19, 2021), https://www.lakshmisri.com/insights/articles/fall-back-liability-under-the-consumer-protection-e-commerce-rules-2020-stricter-norms-in-digital-diaspora/.
[14] Narasimha Raju, *Govt. to Tighten eCommerce Rules*, CXOToday.com (Mar. 23, 2023), https://cxotoday.com/news-analysis/govt-to-tighten-ecommerce-rules/.
[15] Legal Thirst, *KNOW THE CONSUMER PROTECTION ACT & FALLBACK LIABILITY*, Legal Thirst Associates: Consumer Guide (2023), https://legalthirst.com/know-the-consumer-protection-act-fallback-liability/.
[16] INFORMATION TECHNOLOGY ACT, 2000, Law No. ACT NO. 21 2000, June 9, 2000, XXXX (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

wide range of online service providers, thereby encouraging investment and innovation without the chilling effect of constant litigation over user-generated data.

Legislative Purpose and Overriding Effect

Section 79 is a legislative intervention aimed at balancing the regulation of online content with the promotion of internet-based services. The provision begins with a powerful 'non-obstante' clause: "Notwithstanding anything contained in any law for the time being in force...".[17] This phrasing explains a clear legislative intent for Section 79 to have an overriding effect over other laws that might otherwise impose liability on intermediaries for third-party actions. This clause is the textual source of the direct conflict with the liability regime under the CPA 2019.

Definition of 'Intermediary'

The scope of Section 79's protection is defined by the term 'intermediary' in Section 2(1)(w)[18] of the IT Act. This definition is broad, encompassing any person who, on behalf of another, "receives, stores or transmits" an electronic record or provides any service with respect to that record. The definition explicitly includes telecom providers, internet service providers, search engines, and, crucially for this analysis, "online-market places" and "online-auction sites".[19] The inclusion of these terms makes it clear that e-commerce platforms like Amazon and Flipkart were prima facie intended by the legislature to be considered intermediaries and thus be eligible for the safe harbour protection offered by Section 79.

Conditions for Safe Harbour

The immunity granted by Section 79 is not absolute; it is conditional upon the intermediary satisfying a set of stringent requirements laid out in subsections (2) and (3)[20]. These conditions construct a model of a neutral conduit that acts responsibly upon receiving formal notification of illegality.

The first condition requires that the intermediary's role be functionally limited and technically passive. Its function must be limited to "providing access to a communication system," and it

[17] Id.
[18] Id.
[19] Id.
[20] INFORMATION TECHNOLOGY ACT, 2000, Law No. ACT NO. 21 2000, June 9, 2000, XXXX (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

must not "(i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission".[10] This establishes the 'mere conduit' test, where the intermediary is expected to be a neutral facilitator of information, not its creator, editor, or curator. The intermediary must observe "due diligence" while discharging its duties under the Act and must also adhere to guidelines prescribed by the Central Government. These guidelines are primarily encapsulated in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. These rules mandate intermediaries to, among other things, publish their rules and regulations, privacy policy, and user agreement; inform users not to host, display, or share prohibited categories of content; and establish a grievance redressal mechanism for users. The safe harbour protection is forfeited if the intermediary fails to act after gaining knowledge of unlawful activity. Section 79(3)(b) states that the immunity shall not apply if "upon receiving actual knowledge, or on being notified by the appropriate Government or its agency" that its computer resources are being used to commit an unlawful act, the intermediary "fails to expeditiously remove or disable access to that material". The interpretation of "actual knowledge" is critical. In the landmark case of *Shreya Singhal v. Union of India*[21], the Supreme Court of India read down this provision, holding that "actual knowledge" must be construed as knowledge received via a court order or a notification from a government agency. This interpretation protects intermediaries from the impossible burden of adjudicating the legality of millions of user complaints and establishes a high, formal threshold for triggering their takedown obligation.

Active Involvement: Loss of Immunity

In addition to the takedown obligation, immunity is also lost under Section 79(3)(a) if "the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act".[22] This clause is pivotal, as it provides a statutory basis for courts to examine the degree of an intermediary's involvement in the underlying unlawful activity.

The legal architecture of Section 79 thus creates a reactive liability model. It immunizes intermediaries for unlawful third-party activities of which they are unaware and imposes a duty

[21] Shreya Singhal v. Union of India, SUPREME CT. OF INDIA, May 24, 2015, WRIT PETITION (CRIMINAL) NO.167 OF 2012, SCC, at XXXX (India).
[22] INFORMATION TECHNOLOGY ACT, 2000, Law No. ACT NO. 21 2000, June 9, 2000, XXXX (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

to act only after receiving a formal, legally vetted notification of specific illegality. This model is fundamentally at odds with the proactive, guarantor-like role envisaged for e-commerce marketplaces by the 'fall-back liability' clause. Under the IT Act, a platform could be fully compliant with its due diligence and reactive takedown duties and still be protected by safe harbour. However, under the E-commerce Rules, the same platform could be held liable for a seller's negligence based on a mere consumer complaint, without any court order. This direct contradiction places the 'non-obstante' clause of Section 79 on a collision course with the consumer welfare mandate of the CPA 2019.

Interpreting Liability in the Digital Marketplace: The Judicial Dilemma

The inherent statutory conflict between the consumer-centric CPA 2019 and the intermediary-protective IT Act has left the Indian judiciary in an ambiguous position, tasked with applying these contradictory statutes to real-world disputes, courts and consumer forums have developed divergent and often inconsistent lines of reasoning.

The "Objective Approach": Liability Based on Role and Control

The judiciary's inconsistent approach stems from a deeper jurisprudential problem: the very nature of platform liability. In traditional legal theory, liability imposition requires a subjective "fault" on the part of the offender. The IT Act's "actual knowledge" standard reflects this fault-based model. However, the modern digital marketplace, with its anonymity and information asymmetry, creates unique risks for consumers. This has initiated a search for "secondary liability", holding the platform responsible for the "direct infringement" of the seller. In response, courts have developed two distinct rationales for imposing this secondary liability: an "Objective Approach" focusing on the platform's control, and a "Subjective Approach" focusing on the consumer's perception.[23]

The 'Active' vs. 'Passive' Participation Test

The Delhi High Court's 2018 judgment in *Christian Louboutin SAS v. Nakul Bajaj & Ors*. This case involved the sale of alleged counterfeit luxury goods on the e-commerce platform

[23] Dmitriy Kozhemyakin & Svetlana Mironova, *LEGAL APPROACHES TO LIABILITY OF DIGI Y OF DIGITAL PLATFORM OPERATORS TO CONSUMERS*, 10 Int'l J. on Consumer L. & Prac. 2, XXXX (2022), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1076&context=ijclp.

Darveys.com. The platform claimed protection under Section 79 of the IT Act, arguing it was merely an intermediary connecting sellers and buyers.[24]

The Court, however, rejected this defense, introducing a crucial distinction between 'passive' and 'active' intermediaries. It held that the safe harbour provision was intended only for the former. The Court found that Darveys.com was an 'active participant' in the transactions occurring on its platform and was therefore disqualified from Section 79 immunity. Justice Pratibha M. Singh laid down a non-exhaustive list of factors that could indicate such active involvement, moving a platform beyond the role of a mere conduit. These factors included: Providing authenticity guarantees for products; Offering warehousing, packaging, and shipping services under the platform's brand; Managing customer care and handling complaints about product quality; Actively curating or pre-screening product listings; Using the brand's name as meta-tags to drive traffic to the site.[25]

The Court reasoned that such deep involvement in the transaction, from quality assurance to logistics, amounted to "aiding" or "inducing" the commission of the unlawful act (in this case, trademark infringement) under Section 79(3)(a), thereby stripping the platform of its immunity. The *Louboutin* judgment was a landmark decision that significantly narrowed the perceived scope of safe harbour for many e-commerce business models, suggesting that the more value-added services a platform provides, the higher its risk of liability.

The relevance of "Objective Approach" to platform liability is reflected in the above discussed "active vs. passive" test, established in *Christian Louboutin*,. The court's 18-factor list was an attempt to answer one question: does the platform exert "substantial control" over the transaction? This reasoning directly parallels U.S. jurisprudence, such as in *Oberdorf v. Amazon.com Inc.*, where the court imposed liability by reasoning that Amazon's control over sellers,.including its right to remove listings and withhold payments, made it "fully capable... of removing unsafe products" and thus the only party available to the victim for redress. In this objective view, the platform is held liable because its "significant influence" and control make

[24] Aahana Acharya, *CHRISTIAN LOUBOUTIN SAS V. NAKUL BAJAJ & ORS AIRONLINE 2018 DEL 1962*, 2 INT'L J. LEGAL STUD. & SOC. SCIS. [IJLSSS] 1, XXXX (2024), https://ijlsss.com/wp-content/uploads/2024/08/1.-Aahana-Acharya.pdf.

[25] SCGB, *Not all e-commerce websites intermediaries: Analysis of Christian Louboutin v. Nakul Bajaj & Ors.*, SCGB Solutions, https://scgbsolutions.com/not-all-e-commerce-websites-intermediaries-analysis-of-christian-louboutin-v-nakul-bajaj-ors/ (last visited Oct. 29, 2025).

it the most logical and effective entity to manage the risk and not because it was *at fault*.[26]

Reassessing the Boundaries of 'Active' Participation

The strict standard set in *Louboutin* was challenged and arguably diluted by a subsequent Division Bench ruling of the Delhi High Court in *Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors.* (2020). This case concerned the unauthorized sale of products from direct-selling companies like Amway on Amazon's marketplace. The single-judge bench had initially followed the *Louboutin* reasoning, holding Amazon to be an 'active' intermediary due to its involvement in storage, packaging, and delivery, thus denying it safe harbour protection.

However, the Division Bench overturned this finding. It explicitly rejected a rigid 'active' versus 'passive' binary, stating that Section 79 of the IT Act makes no such distinction. The Court held that the provision of value-added services such as warehousing (Fulfilment by Amazon), packaging, and last-mile delivery does not automatically disqualify a platform from its intermediary status. The Court reasoned that such services are integral to the functioning of an online marketplace and are services provided to the seller, not an alteration of the product information itself. The judgment noted that as long as the platform does not initiate the transmission, select the receiver, or modify the content of the information (the core tests under Section 79(2)(b)), it remains an intermediary. This ruling represented a significant pull-back from the expansive liability standard of *Louboutin*, realigning the interpretation more closely with the literal text of the IT Act and reinforcing the safe harbour defense for major e-commerce platforms.[27]

Liability Based on Consumer Perception : The Consumer Fora's Subjective Approach

While the High Courts have debated the nuances of the IT Act, the consumer dispute redressal commissions have adopted a straightforward approach: prioritizing the consumer's right to redressal.

[26] Dmitriy Kozhemyakin & Svetlana Mironova, *LEGAL APPROACHES TO LIABILITY OF DIGI Y OF DIGITAL PLATFORM OPERATORS TO CONSUMERS*, 10 Int'l J. on Consumer L. & Prac. 2, XXXX (2022), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1076&context=ijclp.

[27] Mukul Sharma et al., *Safe Harbour Protection for E-Commerce platforms*, India Corporate Law: cyril amarchand magaldas (July 15, 2021), https://corporate.cyrilamarchandblogs.com/2021/07/safe-harbour-protection-for-e-commerce-platforms/.

In cases like *Amazon Seller Services Pvt. Ltd. v. Gopal Krishan*, the National Consumer Disputes Redressal Commission (NCDRC) held the platform vicariously liable for a defective product, reasoning that an "agent, who sells a product, is duty bound to ensure its quality" and cannot escape liability.[28] More recently, a 2025 ruling by the Chandigarh Consumer Commission in *Supriya Chandra v. Amazon* held the platform "equally liable" for a damaged product delivered by a third-party seller.[29]

This consistent line of reasoning from the consumer commissions grounded in consumer-centric principles is a powerful example of the "Subjective Approach". This approach analyzes liability from the *consumer's perception* of that function and not from the platform's technical function. The forums observe that consumers place their trust not in the unknown but platform's brand and reputation, often unverified third-party seller. As the platform "strives to maximally mediate the communication" and "minimises information about the executor himself," the figures of the platform and the seller "merge together" in the consumer's mind. The Chandigarh Commission's finding that consumers are "attracted... keeping in view the brand name and reputation of the platforms... and not the seller at all" perfectly captures this idea. It mirrors the Danish court's ruling in the *GoLeif.dk* case, where the platform was held liable because it "did not clearly indicate" that the airline was the true service provider, leading the consumer to assume they were transacting directly with the platform.[30] By profiting from this transaction, the platform is seen as an integral part of the service offering and cannot, in the eyes of the consumer courts, simply shift responsibility when a cause of action arises. This perspective aligns perfectly with the spirit of the 'fall-back liability' clause, demonstrating that the judiciary's consumer protection arm already operates on a similar principle of platform accountability.

Collision of Legislative Mandates

The tension between consumer protection and intermediary immunity is a direct clash of

[28] Vidhi Madan, *'Fall-back liability' under the Consumer Protection (e-Commerce) Rules, 2020: Stricter norms in digital diaspora*, Lakshmikumaran & Sridharan: Top Law Firm in India (Oct. 19, 2021), https://www.lakshmisri.com/insights/articles/fall-back-liability-under-the-consumer-protection-e-commerce-rules-2020-stricter-norms-in-digital-diaspora/.

[29] More recently, a 2025 ruling by the Chandigarh Consumer Commission in *Supriya Chandra v. Amazon* held the platform "equally liable" for a damaged product delivered by a third-party seller

[30] Dmitriy Kozhemyakin & Svetlana Mironova, *LEGAL APPROACHES TO LIABILITY OF DIGI Y OF DIGITAL PLATFORM OPERATORS TO CONSUMERS*, 10 Int'l J. on Consumer L. & Prac. 2, XXXX (2022), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1076&context=ijclp.

legislative mandates and not merely a matter of judicial interpretation. The proposed 'fall-back liability' clause under the E-commerce Rules represents the logical means of the CPA 2019's philosophy, while Section 79 of the IT Act embodies a conflicting vision for regulating the digital space. This collision forces a policy debate about the desired role and therby the responsibility of e-commerce platforms in India, presenting arguments for consumer security against concerns for market innovation and growth.

Direct Contradiction in Legal Architecture

Section 79 of the IT Act, with its 'non-obstante' clause, is designed to provide a shield an exemption *from* liability for the actions of third parties, contingent on the platform maintaining a reactive stance. In contrast, the 'fall-back liability' clause is designed as a sword, it imposes liability on the platform for the very same third-party (seller) actions, demanding a proactive or guarantor role. The conflict between the two regimes is irreconcilable at a textual level. There is a potential of legal paradox where adherence to one law does not provide defense under another, leading to profound regulatory uncertainty, as a platform can simultaneously be in full compliance with the due diligence and reactive takedown requirements of the IT Act, thus qualifying for safe harbour, yet be held liable under the E-commerce Rules for a seller's failure to deliver a product.

The Case for Stricter Liability (Pro-Fall-Back Liability)

The arguments in favor of the 'fall-back liability' clause are rooted in principles of consumer welfare, fairness, and the economic realities of the modern digital marketplace.

In an online transaction, the consumer's primary relationship is with the platform. They are drawn in by the platform's marketing, rely on its interface and payment systems, and trust its brand reputation.[31] The third-party seller is often an anonymous, faceless entity with whom the consumer has no direct rapport or effective means of recourse. When a transaction fails, holding the platform accountable provides the consumer with a single, identifiable, and responsible entity against which to seek redress.

Proponents aligns e-commerce marketplaces with the legal principle of vicarious liability,

[31] More recently, a 2025 ruling by the Chandigarh Consumer Commission in *Supriya Chandra v. Amazon* held the platform "equally liable" for a damaged product delivered by a third-party seller

where a principal (the platform) is held responsible for the acts of its agent (the seller), especially when the agent's actions are integral to the principal's business model. They argue that large e-commerce marketplaces are not passive public utilities; they are sophisticated commercial enterprises that actively shape and monetize the entire transaction ecosystem.[32] This profitable involvement makes them more than just intermediaries.

The platform has the resources and data to vet sellers, monitor their performance, implement quality control measures, and insure against defaults and hence is in the best position to manage the risks associated with third-party sellers. The individual consumer possesses none of this power. Imposing fall-back liability correctly allocates the risk to the party best equipped to mitigate it, incentivizing platforms to create a safer and more reliable marketplace.

The Case for Safe Harbour (Anti-Fall-Back Liability)

The arguments against 'fall-back liability' is primarily voiced by industry stakeholders and is based on concerns about economic viability, innovation, and unintended negative consequences for the market ecosystem.

The central argument against this provision is that it would fundamentally alter the business model of online marketplaces, transforming them from technology facilitators into de facto insurers for millions of transactions. This would impose immense operational costs for monitoring, compliance as well as capital requirements to cover liabilities.[33] Critics argue that it is practically impossible for a large marketplace hosting millions of sellers and billions of listings to proactively guarantee the performance of every single transaction A significant concern is the potential harm to Micro, Small, and Medium Enterprises (MSMEs). Faced with the risk of being held liable for every seller's failure, platforms would inevitably become more risk-averse. This would erect significant barriers to entry, undermining one of the key benefits of e-commerce: providing a level playing field and national market access for small businesses.[34] This could lead to reduced competition, less product variety, and higher prices

[32] Dmitriy Kozhemyakin & Svetlana Mironova, *LEGAL APPROACHES TO LIABILITY OF DIGI Y OF DIGITAL PLATFORM OPERATORS TO CONSUMERS*, 10 Int'l J. on Consumer L. &
Prac. 2, XXXX (2022), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1076&context=ijclp.
[33] Vasundhara Majithia, *The Changing Landscape of Intermediary Liability for ECommerce Platforms: Emergence of a New Regime*, 15 Indian J.L. &
Tech. 8, XXXX (2019), https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1021&context=ijlt.
[34] Aruna Sharma, *Fallback liability: Why holding online marketplaces responsible for consumer protection may harm MSME growth*, Econ. Times, May 3, 2023, https://economictimes.indiatimes.com/small-biz/sme-

for consumers

Major industry bodies like NASSCOM have strongly advocated against a blanket liability rule, suggesting that any such liability should be limited to ensuring timely refunds or linked to specific guarantees expressly made by the platform.[35] This debate is not just external; it reflects a policy schism within the Indian government itself. Reports have indicated that bodies like the Niti Aayog have raised concerns that the proposed E-commerce Rules are overly stringent and could stifle the industry, suggesting that the drive for consumer protection may be at odds with the government's other goals of promoting digital growth and ease of doing business. This reveals that the conflict is not just between two laws, but between two competing visions for the future of India's digital economy.

Lessons from Abroad: A Comparative Analysis of Global Liability Regime

The regulatory challenge facing India is not unique. Jurisdictions around the world have grappled with the question of how to hold online platforms accountable without stifling the digital economy. Examining the approaches taken by tthe European Union provides valuable context and reveals potential pathways for resolving India's legislative conflict

Conditional Immunity and Co-Regulation- E.U Approach

The European Union offers a balanced regulatory model, recently updated through its landmark Digital Services Act (DSA). This framework preserves the core principle of conditional safe harbour but significantly strengthens the due diligence obligations required to earn that protection.

The DSA, which builds upon the foundational E-Commerce Directive, creates a comprehensive regulatory framework for online intermediaries. It maintains the conditional liability exemption: a hosting service is not liable for illegal content stored at the request of a user, provided it does not have "actual knowledge" of the illegal activity and, upon obtaining such knowledge, "acts expeditiously to remove or to disable access to the content". The DSA's most significant innovation for e-commerce is the introduction of stringent 'Know Your Business

sector/fallback-liability-why-holding-online-marketplaces-responsible-for-consumer-protection-may-harm-msme-growth/articleshow/99952675.cms?from=mdr.

[35] PTI, *E-comm rules: Nasscom says rationalise obligations based on activities, limit fallback liability to timely refund.*, Times India, July 23, 2023, https://timesofindia.indiatimes.com/e-comm-rules-nasscom-says-rationalise-obligations-based-on-activities-limit-fallback-liability-to-timely-refund/articleshow/84673742.cms.

Customer' (KYBC) obligations for online marketplaces, as detailed in Article 30. Before allowing a third-party seller (or 'trader') to offer goods or services to EU consumers, a marketplace must collect, verify, and make reasonable efforts to assess the reliability of essential information from that seller. This includes the seller's name, contact details, a copy of an identification document, payment account details, and their trade register number, if applicable. The DSA further mandates 'compliance by design' (Article 31), requiring marketplaces to design their interfaces in a way that enables sellers to comply with their own legal obligations regarding product information and safety. Furthermore, under the 'right to information' (Article 32), if a platform becomes aware that an illegal product has been sold, it must inform the consumers who purchased it about the illegality and any available means of redress.[36]

The EU's approach intends a 'middle path'. It avoids the absolutism of the India's proposed 'fall-back liability'. The DSA significantly raises the bar for due diligence, without making the platform a guarantor for every transaction. The safe harbour is not an absolute right but a privilege that must be earned through proactive and risk-mitigating measures. This model directly addresses the core problem of anonymous and potentially fraudulent sellers that plagues online marketplaces. It suggests a viable direction for India: rather than creating a new, conflicting liability rule in the E-commerce Rules, the more coherent approach would be to amend the IT Act's Intermediary Guidelines to incorporate stronger, DSA-style due diligence obligations as a prerequisite for claiming Section 79 protection in the specific context of e-commerce.

Towards a Coherent and Balanced Regulatory Framework

The prevailing state of regulatory conflict and judicial inconsistency surrounding the liability of e-commerce marketplaces in India is untenable. The direct collision between the consumer-centric 'fall-back liability' regime of the CPA 2019 and the intermediary-protective 'safe harbour' of the IT Act creates significant legal uncertainty. This ambiguity not only undermines investor confidence and complicates business operations but also fails to provide a clear, predictable framework for either consumers or platforms.[83] To foster a sustainable and

[36] Latham & Watkins LLP, *The Digital Services Act: Practical Implications for Online Services and Platforms*, Latham & Watkins LLP | Global Law Firm (Mar. 2023), https://www.lw.com/admin/upload/SiteAttachments/Digital-Services-Act-Practical-Implications-for-Online-Services-and-Platforms.pdf

trustworthy digital economy, a harmonized approach is imperative. This requires a concerted effort across legislative, judicial, and policy domains to reconcile these competing mandates.

Legislative Pathways

The most effective and durable solution lies in legislative reform that directly addresses the source of the conflict. The goal should be to create a single, coherent set of rules for e-commerce intermediaries that balances accountability with feasibility.

The most logical pathway is to amend the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules to introduce a specific category for 'e-commerce marketplace intermediaries'. This would allow for the creation of a bespoke due diligence framework tailored to the unique risks of online retail, without dismantling the broader safe harbour principle of Section 79. Inspired by the EU's Digital Services Act, these heightened due diligence requirements should include:

Requiring platforms to collect and verify essential identity and contact information from all sellers before allowing them to list products. This would directly combat the issue of anonymous and fraudulent sellers. Mandating that platforms obtain legally binding undertakings from sellers that they will comply with all applicable laws, including consumer protection, legal metrology, and intellectual property rights. Requiring clear disclosure of seller details on product listings and an explanation of the platform's role in the transaction (e.g., whether it provides logistics, warehousing, or quality checks).

By making Section 79's safe harbour conditional upon adherence to these stricter, sector-specific due diligence norms, the law would create a powerful incentive for platforms to build safer marketplaces. The safe harbour would become a privilege to be earned through responsible governance, not an automatic right.

However, this legislative pathway must be navigated with extreme caution, as it is part of a broader, problematic regulatory trend. The 2025 draft amendments concerning AI-generated content, for example, use the exact same legal mechanism as the 'fall-back liability' clause: they attempt to bypass the reactive "actual knowledge" standard set by *Shreya Singhal* by imposing a proactive, automated *duty to verify*. This approach effectively redefines "due diligence" as the successful operation of a proactive monitoring architecture. This not only inverts the

purpose of safe harbour from a shield into a "sword" of enforcement but also creates a "chilling effect." In the case of the AI rules, it threatens free expression; in the case of 'fall-back liability', it would create a devastating "chilling effect on commerce," as platforms would be forced to purge thousands of small MSMEs to avoid liability. [37]

Therefore, any new "bespoke due diligence framework" for e-commerce must be carefully ring-fenced.

If policymakers choose to proceed with the 'fall-back liability' clause, it must be significantly clarified to avoid an absolutist interpretation. The judiciary could be guided to read down the provision, applying it not as a blanket rule of vicarious liability but as a measure of last resort in specific cases where a platform has demonstrably failed its fundamental due diligence obligations. Alternatively, as suggested by industry bodies, its scope could be statutorily limited to ensuring that the platform guarantees a timely refund to the consumer in case of non-delivery or seller default, without extending to broader consequential damages.

Conclusion

Indian e-commerce regulation has to be advertent so as to not make a binary choice between innovation and absolute consumer protection. The goal must be to create a regulatory environment which becomes a means where these two objectives are mutually reinforcing. A marketplace that consumers trust will ultimately persist and thrive. The uncertainity created by current legal conflict leaves accountability gaps thereby undermining the ‘trust’. A harmonised framework built on the principle of enhanced transparency, proactive and reasonable due diligence, and shared responsibility offers the most sustainable path forward. By placing clear obligations on platforms to know their sellers, on sellers to be accountable for their products, and by strengthening the right to information of the consumers, India can build a digital economy that is in addition to being robust and innovative is also safe, fair, and equitable for all its participants.

[37] Sumukhi Subramanian, *Decoding the proposed IT Amendment Rules, 2025*, The Leaflet: Law and Technology (Oct. 24, 2025), https://theleaflet.in/digital-rights/law-and-technology/decoding-the-proposed-it-amendment-rules-2025.