The Dialogue™
INFORM ENGAGE IDEATE

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

White Paper

ADVANCING THE DIGITAL ECONOMY

Shaping the E-Commerce Regulatory Landscape

8th April 2022

AUTHORS

The Dialogue™

- Kazim Rizvi
- Ayush Tripathi
- Eshani Vaidya

Nishith Desai Associates

- Gowree Gokhale
- Meyyappan N
- Aaron Kamath
- Inika Charles
- Vibhore Batwara
- Ipsita Agarwalla

Copyedited By: Kriti Singh

Designed By: Diksha Kumari

ABOUT THE ORGANISATIONS

The Dialogue™
INFORM ENGAGE IDEATE

The Dialogue™ is a public-policy think- tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think- tanks to watch out for, by the Think-Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

At Nishith Desai Associates, we have earned the reputation of being Asia being most Innovative Law Firm – and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bangalore, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly – the VISION – to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of things (IoT), Aviation Artificial Intelligence, Privatization of Outer Space, Drones, Robotics Virtual Reality, Ed-Tech, Med-Tech & Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

NDA has been the proud recipient of the RSG – FT award for 2019, 2017, 2016, 2015, 2014 as the 'Most Innovative Indian Law Firm' and in 2016 we were awarded the 'Most Innovative Law Firm – Asia Pacific,' by Financial Times (London).

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

TABLE OF CONTENTS

I. Executive Summary

E-commerce is rapidly taking up space in India's economic growth. With a huge market potential because of the wide consumer base, India presents itself as an attractive destination for e-commerce entities, both domestic and foreign. At the same time, traditional brick and mortar businesses are also using online sales as one of the key distribution channels. These evolving business models require a suitable environment to foster their growth. In India, regulators have unfortunately adopted a one-size-fits-all policy to regulate e-commerce entities, which has led to over regulation in some instances, as we highlight through the paper.

We note that across regulations, any entity with an online presence may get covered under the term "e-commerce". With business models evolving, there is a greater need for exclusivity in terms of what is and is not classified as e-commerce. The current regulatory architecture is not flexible enough to accommodate newly emerging business models, which leads to barriers of over regulation in their growth.

There are myriad laws applicable to the e-commerce entities, including but not limited to -- consumer protection, food laws, legal metrology laws, intermediary liability, payment laws, data protection, taxation, competition law, etc. which have been summarily described in Chapter III, and explained in detail in Annexure I. Multiplicity of regulations and regulators hampers the growth of the ecosystem.

Each of these laws provide different definitions, approaches, and obligations on e-commerce entities. In Chapter II, we specifically discuss the business models that are covered under the current definition of e-commerce. The government could consider providing definitions based on the object of each regulation and specifically carve out those models which are not relevant for that particular regulation.

Compliance obligations may be imposed according to the regulations based on the size, impact, business model, functionality and role played by each stakeholder. As a result of the broad definitions and undefined scope, there has been significant ambiguity in the application of these laws. A prime example is of the Equalisation Levy 2020, which was criticised for being too broad. Similarly, the proposed amendments to consumer protection e-commerce rules also came into the scanner for including the whole supply chain under the definition of e-commerce. For example, logistics should not be the responsibility of e-commerce entities. Similarly, creating a fall back liability for negligence of sellers also does not seem to be the correct approach. Therefore, 'e-commerce' must be clearly defined. At the very least, the definition must expressly provide for entities that are not to be classified as e-commerce.

It is important to revisit the legal obligations to make the ecosystem more inclusive and to ease the entry for new e-commerce entities. Regulations should not act as an entry barrier. As we have covered in detail in Chapter IV, significant parts of the industry appear to be over-regulated. There is a need to clarify the applicability of relevant law for different business models in the e-commerce industry.

Challenges relating to consumer protection, especially the proposed amendments in June 2021, pose a serious threat to the growth of domestic online marketplace entities as it creates significant compliance burden and imposes liabilities. Further, there are several challenges relating to the operational tax regime for e-commerce. Section 194-O of Income Tax Act, 1961, owing to its broad nature, covers a wide range of businesses which may not be a part of transactions such as third party apps, in which a transaction is happening between a buyer and a seller or a secondary website taking you to the primary e-commerce website for final transactions. Similarly, disparity in Goods and Services Tax (GST) between

online and offline modes also need to be reconsidered to make it easy for the companies to operate in this space. India's FDI policy is another issue that needs rethink. Issues relating to sale of third party sourced goods and definition of marketplace and policies around single brand and multi brand retailing needs further consideration in order to foster e-commerce growth.

Further, the sheer number of sectoral regulators is another aspect to look at. With multiple regulators such as Telecom Regulatory Authority of India (TRAI), Competition Commission of India (CCI), Ministry of Electronics and Information Technology (MeitY), Department for Promotion of Industry and Internal Trade (DPIIT), and Consumer Protection Act (CPA) controlling different, and often overlapping aspects of e-commerce, which may lead to regulatory arbitrage. Upon enactment of a Data Protection Bill and the Data Protection Authority, it is likely that this scenario will get more complicated.A detailed set of policy challenges are enumerated in Chapter VI.

This report further delves into the question of how other countries are regulating the e-commerce space. The study brings in perspectives from the US, UK, EU, and Australia to explore how they are regulating the digital space. Chapter V is dedicated to the international best practices to understand regulation from a global perspective.

In order to develop an enabling ecosystem, regulations must not only benefit the consumer but also encourage innovation within this sector. As discussed in the report, eliminating onerous compliance obligations is essential to minimise bureaucratic delays and operational costs. There is a need to harmonise the laws governing e-commerce as different regulations offer different regulatory scope and there is no uniform applicability of laws. A uniform regulatory approach with lesser compliance would give India's digital companies an environment of ease of doing business and encourage them to grow and innovate.

It must be noted that regulation cannot be created in a vacuum. Developing an open, consultative and participatory process will allow a dynamic ecosystem that should reflect in the laws. An inclusive, stakeholder-driven process will allow regulation to effectively address individual concerns and sectoral peculiarities.

Way Forward

01 Provide for a definition for 'e-commerce' entities, which should carve out exceptions within it.

02 Adopt a light-touch regulatory approach by way of eliminating onerous compliance burdens.

03 Develop a co-regulatory approach in order to prevent regulatory arbitrage.

04 Develop a participative and open consultative process in order to formulate effective and inclusive regulation.

01. Introduction

As India begins to augment its information technology prowess, it is keen to advance its digital economy, driven by new technologies and innovations. In the COVID-19 hit world, e-commerce has emerged as one of the important factors for the growth of the economy and the sustenance of businesses. E-commerce, which has fuelled digital economies globally, has not reached its true potential in India yet. In recent years, it has helped local artisans and small sellers to directly sell their products to consumers at fair prices, minimising the role of middlemen. The existing regulatory arbitrage has been one of the major factors which has impeded the growth of entities in the sector. Given that India has set a goal of becoming a trillion dollar digital economy, it is imperative that focus must be given to this major aspect of the digital[1] sphere.

The e-commerce market has grown multifold in the past few years with a market size of USD 9.09 trillion globally in 2019. In India, this market size was USD 46 billion in 2020 with the projection of reaching[2] almost USD 200 billion by 2027. Further, India's average e-commerce revenue per user was around $50[3] per year in 2018, a figure that must grow significantly to match global standards. The Asian market[4] contributes 62.6% of the total sales revenue generated from e-commerce ventures, which makes it the most lucrative geographical region. Currently, China leads the world in digital buyers in 2021 with 792.5 million users (33.3% of the global total) . Due to increased digitisation, e-commerce in other South Asian[5] countries such as Indonesia, Malaysia, Philippines, Singapore, Thailand, and Vietnam is also growing exponentially. In order to maximise on the potential of the e-commerce sector and effectively compete at the global stage, it is important that India develops an enabling regulatory environment.

Towards this, the study seeks to contribute to the discourse to overhaul the regulatory framework of the e-commerce ecosystem in order to keep up with the pace of the emerging digital landscape. **Chapter II** dissects the different businesses operating on the internet to show the diversity in functionality in each of the models. **Chapter III** identifies the current regulatory landscape of e-commerce in India. **Chapter IV** analyses the obligations that should be applicable on the e-commerce entities in order to develop an enabling regulatory environment. **Chapter V** delves into the regulatory framework from major countries. **Chapter VI** evaluates the existing policy challenges in the ecosystem and lastly, **Chapter VII** aims to provide the way forward for India to tap the potential of the digital market.

[1]Ministry of Electronics and Information Technology. (2019). India's *Trillion-Dollar Opportunity*. https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[2]Grand View Research. (2020). E-commerce Market Size, Share & Trends Analysis Report By Model Type (B2B, B2C), By Region *(North America, Europe, APAC, Latin America, Middle East & Africa*), *And Segment Forecasts, 2020 - 2027*. https://www.grandviewresearch.com/industry-analysis/e-commerce-market

[3]Statista. (2021). *India e-commerce market size.* https://www.statista.com/statistics/792047/india-e-commerce-market-size/

[4]The National Association of Software and Service Companies. (2020). Ecommerce in India - Fuelling A Billion Digital Dreams. https://nasscom.in/knowledge-center/publications/ecommerce-india-fuelling-billion-digital-dreams-0

[5]Cramer-Flood, E. (2021). *Global Ecommerce Update 2021: Worldwide Ecommerce Will Approach $5 Trillion This Year. eMarketer.* https://www.emarketer.com/content/global-ecommerce-update-2021; China will produce $2.779 trillion in ecommerce sales (56.8% of the global total); and it will become the first country in history to transact more than half of its retail sales digitally (52.1%).

02. Dissecting Internet Businesses

Over the course of the last decade, different and novel business models have evolved in the digital ecosystem. The widespread adoption of Information and Communication Technology along with the growth in competition, innovation, internet penetration and smartphone availability, have led to new and distinct businesses which are often interconnected in the ecosystem. However, they work on different paradigms and operate for different purposes. It is important to understand that the 'one-size-fits-all approach' for regulating e-commerce might not work in the evolving landscape of the digital economy and e-commerce is one such sector which has faced the brunt of this approach.

It needs to be understood that there are multiple activities happening in the online space, within which some may fall in the e-commerce domain and some may not. There is a need to revisit the definition of e-commerce to exclude businesses which may not be considered as 'e-commerce' because the services that they offer vary, sometimes significantly. For example- while a content streaming platform and a marketplace selling goods both offer services to users, the nuances of their business models need to be considered, and they should not be subject to identical regulations. Instead, business models ought to be regulated based on the dominant activity, which would help to categorise similar business models which may be regulated in a similar manner.

Currently, varying regulations provide different definitions of e-commerce and related concepts. If we look at some of the definitions in the Indian context, per the Consumer Protection (E-commerce) Rules 2020, an e-commerce entity has been defined as "*any person who owns, operates or manages digital or electronic facility or platform for electronic commerce, but does not include a seller offering his goods or services for sale on a marketplace e-commerce entity*."[6] On the other hand, the Finance Act, 2020 defines an e-commerce operator as someone who "*operates or manages digital or electronic facility or platform for online sale of goods or online provision of services or both*."[7] While the former definition carves out the exception for sellers, the same has not been carved out for the latter. Further, *prima facie*, these definitions are over broad and may include any and all online activities without considering the functionality and operational parts of the businesses. Depending upon the purpose of the legislation and the business model sought to be regulated, the definitions should be adapted, which may also clearly carve out some of these business models that are not intended to be covered by the relevant regulation.

E-commerce has been seen as a big umbrella under which different business models such as payments, aggregators, advertisements, etc. operate. The digital services described below have been categorised under three broad heads: Business to Business, Business to Consumer and Consumer to Consumer. It is important to note that the activities listed below may not necessarily be classified as e-commerce. However, the regulatory approach today is such that it brings all these activities under an umbrella regulation for e-commerce.

[6]Rule 3(b), The Consumer Protection (E-Commerce) Rules, 2020

[7]Section 164 (ca), The Finance Act, 2016.

2.1. Business-to-Business Model (B2B)

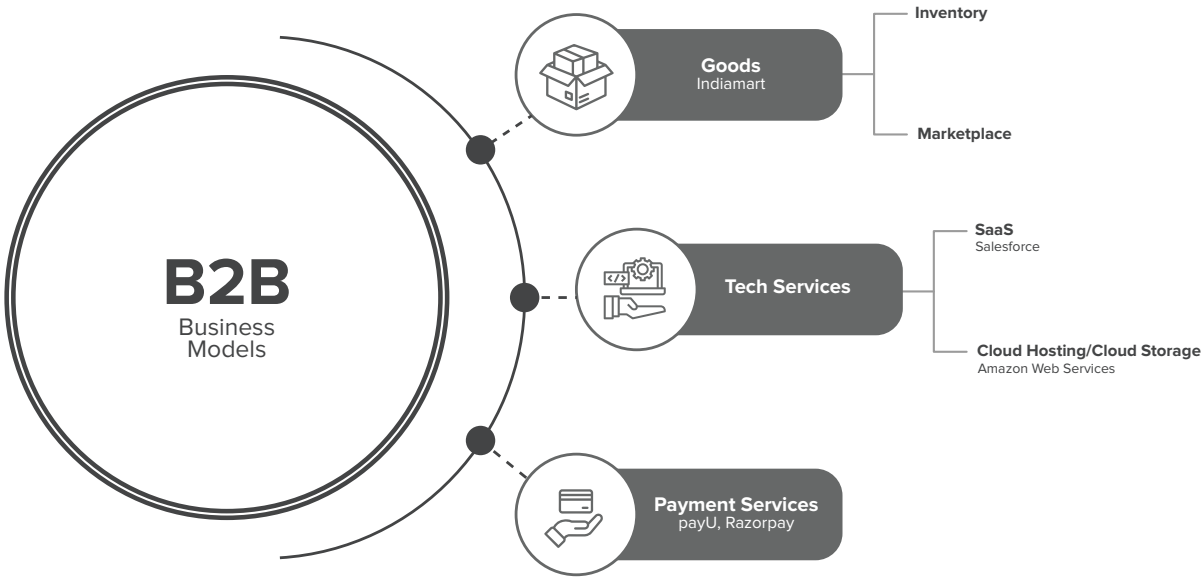

Fig. 1- Examples of B2B Business Models

A B2B model envisages a transaction between two or more businesses the sale or provision of goods or services. In this model, the buyer is not a consumer but the objective of the transaction is either onward selling or utilisation of finished goods/services that are ultimately sold to consumers. Acknowledging the untapped potential of such entities, the Government has allowed 100% FDI in B2B e-commerce, which has attracted companies such as Walmart and Alibaba to invest in the Indian B2B e-Commerce industry.[8] There may be more entry barriers in the B2B compared to the B2C (Business-to-Consumer) industry because a B2B company needs a long term logistical arrangement with rail, road and ports and also adheres to stringent regulatory and taxation requirements.[9]

B2B entities may be of the following types:

1. Goods

i. Inventory

Where platforms maintain an 'inventory' of products that are directly sourced from brands and sellers and sold to retailers or manufacturers. Brands may sell their products directly to other businesses as well.

ii. Marketplace

This model creates a platform that allows discovery of buyers and sellers and for them to interact with one another. Under the B2B model, the two parties between which transactions are facilitated are businesses who tend to purchase products in bulk. IndiaMART is an example. The platform owner charges a commission for this service and is restricted to acting as a facilitator between the two parties.

[8]Ministry of Food and Industry. (2019, December 11). *E-Commerce Business Model* [Press Release]. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1595850

[9]Confederation of Indian Industry. (2016). *e-Commerce in India: A Game Changer for the Economy*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-e-commerce-in-india-noexp.pdf

2. Tech Services

Some services are commonly used to support e-commerce entities and are ancillary services, which may come under the ambit of e-commerce as well.

i. SaaS

Software as a Service (SaaS) is a mode for delivering software to other businesses to carry out certain functions such as customer relationship management (CRM), employee communications, etc. Examples include Salesforce, Dropbox and Adobe.

ii. Cloud Hosting/Storage

Cloud hosting is a business in which services are offered to host websites, applications or data using cloud services. Similarly, in cloud storage, businesses provide a fixed space on their server to host the data or backups of other businesses. Examples include Amazon Web Services (AWS), Bluehost and IBM.

3. Payment Services

Payment service providers, either payment aggregators or payment gateways, provide services to another business to carry out transactions on its website. They enable the merchants to collect payment through debit cards/credit cards/net banking, UPI, etc. Businesses could also provide tech solutions to the online merchants for regular check on their payment mechanisms. Examples include PayU and Razorpay.

2.2. Business to Consumer (B2C)

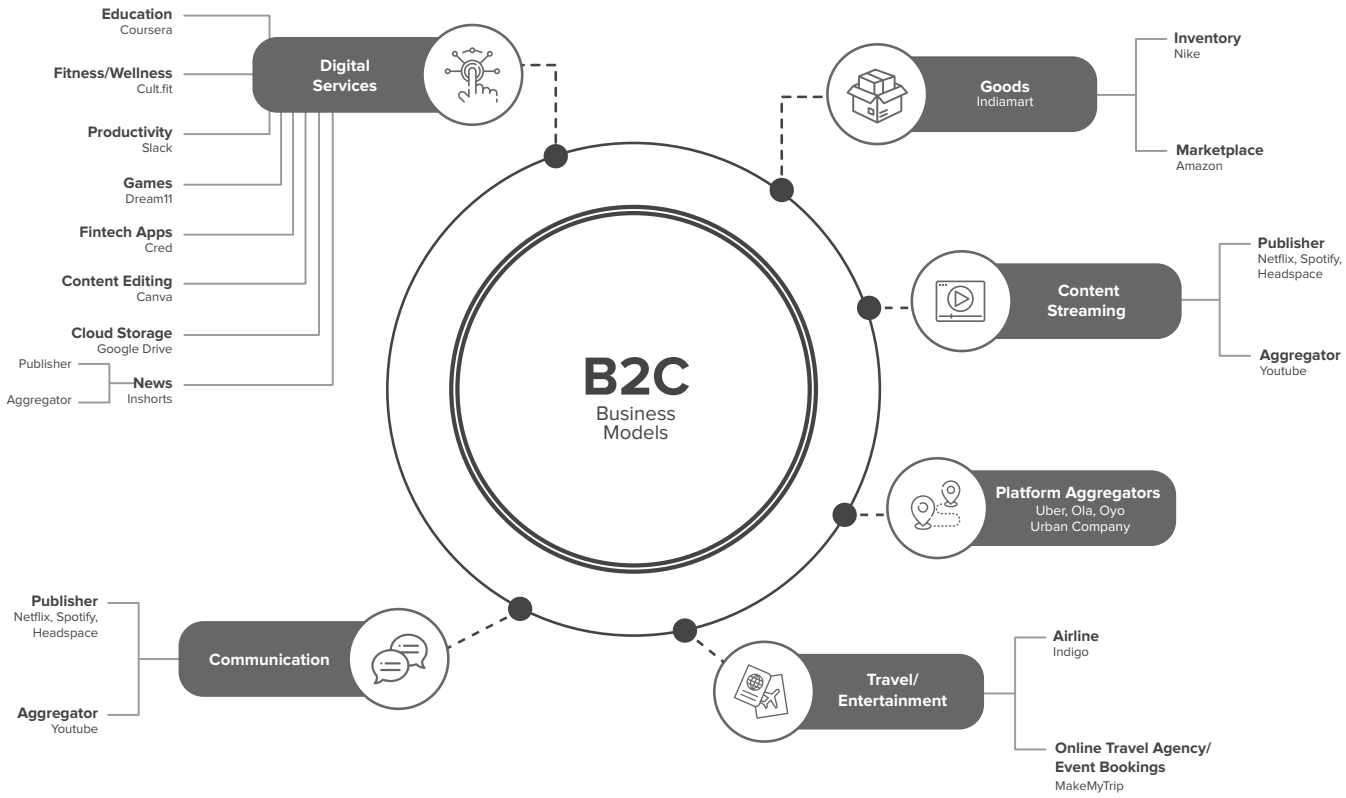

Fig. 2 - Examples of B2C Business Models

The traditional channel of B2C commerce involves the distribution of products through the manufacturer and distributor before it reaches the consumer through the retailer. However, in this model, the merchant can directly deal with the consumer. Therefore, the consumer can place orders directly on the merchant's website, without the utilisation of middlemen.

1. Goods

i. Inventory

Here, the seller holds an inventory of products that it seeks to sell directly to end customers through its own website. Examples include Decathlon, Nike, Adidas etc. This model can be adopted by all entities in the supply chain.

ii. Marketplace

A marketplace platform simply facilitates transactions between the buyers and sellers. Marketplaces onboard third-party sellers who act as a bridge between sellers and the end consumers. Herein, the dominant activity is that of platforms acting as a facilitator between businesses and buyers. The inclusion of platforms that do not facilitate the sale/transactions on their platforms and merely act as catalogues should not be considered as a marketplace. Examples of marketplace includes - Amazon, Flipkart, Snapdeal, Myntra, etc.

2. Content Streaming

Content Streaming platforms allow customers to consume their preferred video content either free or by opting for different modes of payments based on the benefits involved depending on the nature of the platform. Examples of revenue models for consumption of online video content include Subscription Video on Demand (SVOD), Advertisement Supported Video on Demand (AVOD), Transactional Video on Demand (TVOD) and Free Video on Demand (FVOD).

3. Travel/Entertainment

Platforms that sell tickets to their services, such as airline tickets or movie tickets may be categorised as travel/entertainment e-commerce sites. The business either sets up an independent platform or can also be a part of aggregator platforms that host several similar businesses. For example, MakeMyTrip allows the user to book airline or bus tickets.

4. Digital Services

These platforms directly interact with and offer services to the end-user. These include, but are not limited to, EdTech (such as Coursera, platforms for online classes), fitness or wellness services such as wearable trackers, e-sports, fintech, content editing services, and several others.

5. Communication

Any and all services that allow users to communicate with one another in the digital space may also fall within the broad category of e-commerce as they provide services to users.

i. Free

The most common of free communication businesses include social media applications such as Facebook, Snapchat etc, to allow the flow of messages. Similarly, services such as e-mail providers, certain online databases of research material etc. would all be classified as 'free of cost' services available to users.

ii. Freemium

Canva, Discord and other content based communication applications are good examples of the freemium model that allow for access to exclusively paid additions to the base app.

6. Platform Aggregators (B2B+B2C)

An aggregator business model runs as a platform that is owned and managed through a software application offering the services of different service providers of a particular industry under a single brand name. For example, bringing various taxi drivers and offering their services to a consumer through a single application that operates under a particular brand name. Therefore, the aggregator acts as the bridge between the customers and the service providers. There are various brands such as Uber, Ola, Airbnb, Oyo, Urban Company, Zomato etc. operating under this model. The aggregator business model runs on partnership between the aggregator and the service provider, without any terms of employment and only on a contractual basis.

2.3. Consumer to Consumer (C2C)

These platforms allow consumers to interact with one another without the involvement of any third party. OLX and Quikr, for example, allow consumers to trade and purchase items simultaneously. The entity only provides a platform for this exchange, while the delivery etc., is taken care by the users themselves.

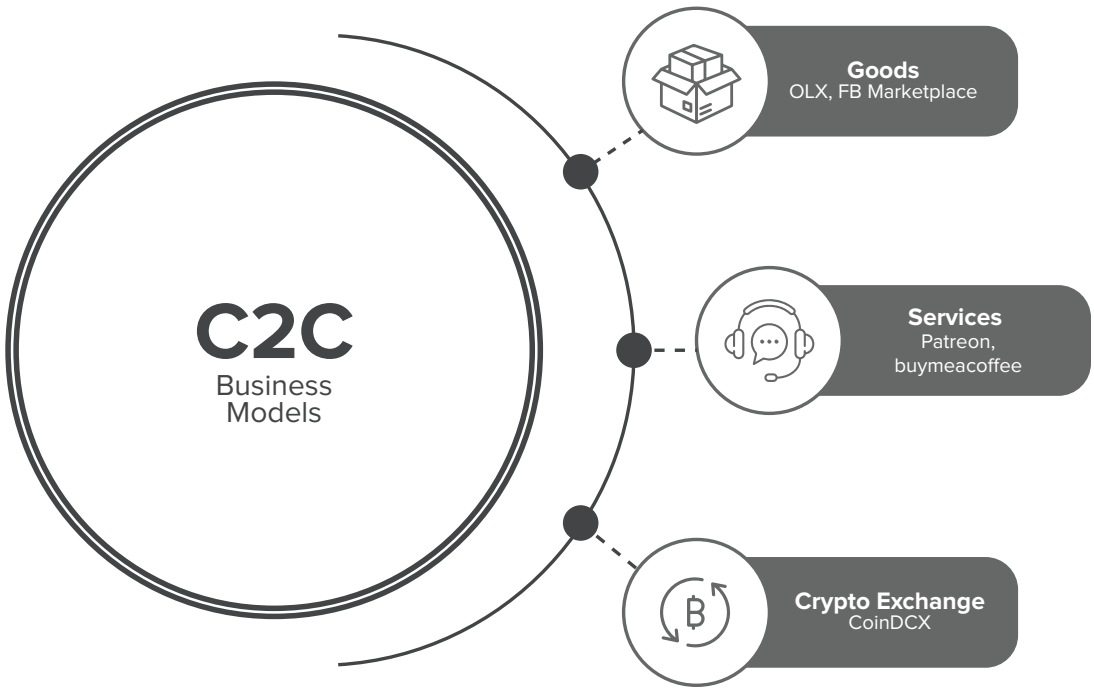

Fig. 3: Examples of C2C Business Models

1. Goods

As discussed earlier, goods-based C2C platforms enable the sale of goods between users. They host advertisements uploaded by users on the website to market goods to other interested users. Examples of this can be seen on OLX. When these platforms allow bulk sales or sales of industrial equipment, they can be termed as 'Hybrid' – an example of this can be seen on Alibaba's platform.

Social media models have also evolved to include C2C marketplaces. Platforms such as FB marketplace are used by users to interact with one another and on their own handle the journey of completion of the transaction off the platform e.g. payment, delivery etc. The platform does not play any role in this transaction.

2. Services

These platforms enable users to distribute content to other consumers exclusively for a fee. In simpler terms, this can be understood as an online platform that helps people freelance their services. (Patreon, buymeacoffee)

3. Crypto exchanges

An exchange platform that allows for the trade in cryptocurrencies and digital assets between consumers similar to how traditional stock markets function.

The following is a summary table for identifying different business models:

Model	Who are you? (B/C)	Who are you selling to? (B/C)	What are you selling? (goods, services, experiences)	How are you selling it? (MLIS/contract-based)	Revenue Model (contract based/ T/S/Ad)
Inventory	Business	Business/Consumer	Goods/Services	* platform owns the inventory of goods logistics/inventory/ Point of Sale	Transaction-based (sales)
Marketplace	Business	Business/Consumer	Goods/Services	Point of Sale	Transaction-based (commission on sale)
Software as a Service (SaaS)	Business	Business	Services	Contact-based	Transaction-based
Cloud-hosting/storage	Business	Business	Services	Contact-based	Transaction-based
Analytics	Business	Business	Services	Contact-based	Transaction-based
Payment Services	Business	Business	Services	Contact-based	Transaction-based
Content Streaming	Business	Consumer	Services	Point of Sale	TVOD (Transaction-based Video on Demand) /SVOD (Subscription-based Video on Demand) /Freemium/ AVOD (Advertisement-based Video on Demand)
Travel/Entertainment	Business	Consumer	Services	Point of Sale	Transaction-based

Model	Who are you? (B/C)	Who are you selling to? (B/C)	What are you selling? (goods, services, experiences)	How are you selling it? (MLIS/contract-based)	Revenue Model (contract based/ T/S/Ad)
Travel/Entertainment	Business	Consumer	Services	Point of Sale	Transaction-based
Digital Services (interactive)	Business	Business/Consumer	Services	Point of Sale	Transaction-based/ Subscription-based
Data licensing	Business	Business	Digital Goods (databases are "literary work" under the Copyright Act, 1957)	Licensing/sub-licensing i.e. contract-based	Contract-based
Platform Aggregators	Business	Consumer	Services	Logistics/Point of Sale	Transaction-based
User Generated Content	Consumer	Consumer	Goods/Services/Exp.	Manufacture/Logistics/Inventory/Point of Sale	Transaction-based

03. Key Regulations Impacting E-commerce

There are a host of regulations that may become applicable to the e-commerce sector. As explored in this paper, e-commerce is a vast sector, home to multiple subsets that cannot necessarily be placed in the same prescriptive box or governed by the same straightjacket compliance requirements.

In **Annexure A**, we have set out a detailed guide to the myriad of laws that may apply to the e-commerce sector. These laws, in summary, are as follows:

Consumer Protection

The Consumer Protection Act, 2019, along with the relatively recently notified the *Consumer Protection (E-Commerce) Rules, 2020* **(Hereinafter "the E-commerce Rules")** prescribe detailed compliance requirements for e-commerce entities engaged in both the 'inventory' and 'marketplace models'. These rules expressly apply to all e-commerce entities operating in India, including entities that are not established in India, yet systematically offer goods or services to consumers in India. Sellers on online marketplaces are also covered under these Rules. There have been few judicial challenges against provisions of these E-commerce Rules, which are still pending. In June 2021, certain amendments were proposed to these rules (**Hereinafter "proposed amendments**"), which sought to broaden the compliance requirements on e-commerce entities. These amendments are still under consideration, and were widely criticised by the industry, civil society organisations, and most importantly by NITI Aayog[10], a government-run think tank.

Intermediary Rules

The *Information Technology [Intermediary Guidelines and Digital Media Ethics Code] Rules, 2021 were notified in February 2021*. These rules expand the scope of due diligence and compliance requirements on intermediaries and introduces obligations on publishers in relation to online content (including news/current affairs and curated content). In response to the feedback that the rules lacked clarity, the MietY released FAQs clarifying certain aspects of the law in November 2021. There have been a number of judicial challenges to these rules, wherein the High Courts of Madras, Bombay and Kerala have issued stay orders on certain provisions of the rules. A challenge to these rules is currently pending before the Supreme Court of India.

Payment Laws

E-commerce platforms that allow users to make and receive payments through their platforms require support from payment gateways and payment aggregators, and in certain instances, may offer either closed or semi-closed pre-paid instruments, such as customer wallets. The Reserve Bank of India (RBI) regulates payment systems through the Payment and Settlement Systems Act, 2007, and has introduced a number of regulations governing entities in the payment ecosystem. These regulations provide for Payment Aggregators to be registered with the RBI, and certain forms of Pre-Paid Instruments to seek authorization with the RBI. Closed loop wallets are not required to be authorised. These regulations also prescribe restrictions on the storing of card data, and for data localisation requirements in certain forms of payment system data. There have also been recent contested circulars on tokenisation and recurring transactions.

[10]Bureau, ET. (2021, August 29). NITI Aayog rejects key parts of ecommerce draft rules. *The Economic Times*. https://economictimes.indiatimes.com/industry/services/retail/niti-aayog-rejects-key-parts-of-ecommerce-draft-rules/articleshow/85727989.cms?from=mdr

Data Protection

The general data protection law in India currently consists of the *Information Technology Act, 2000* (**Hereinafter "IT Act**") and the *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (**Hereinafter "Privacy Rules**"). The IT Act and the Privacy Rules apply to personal data that is collected in or subsequently converted into electronic form. The Privacy Rules require companies, firms, or corporate entities that collect, process and store certain forms of sensitive personal data or information[11], to comply with certain requirements, including obtaining consent, providing notice, maintaining a privacy policy, appointing a grievance officer, and adopting reasonable security measures to protect the information.

In addition to the IT Act and Privacy Rules, there are also certain industry/sector-specific data protection obligations and requirements that may apply, such as in the telecommunications, medical, banking and finance, capital markets, and insurance sectors.

In August 2017, the Supreme Court of India ruled in *Justice K.S. Puttaswamy (Retd.) v. Union of India* that privacy is a fundamental right of an individual enshrined in the Constitution. This led to the formulation of a draft Personal Data Protection Bill 2019 (**Hereinafter, "Proposed Law**")[12], The Proposed Law was referred to a joint parliamentary committee for further debate and examination which presented its report on the Proposed Law in Parliament in December 2021. It recommended several changes to the Proposed Law including broadening its scope to include non-personal data, and renaming the Proposed Law to the Data Protection Bill, 2021. Reportedly, the Government is also currently preparing a draft e-commerce policy that may have provisions about data transfer issues, including provisions regarding the government requests for data.[13]

Taxation Laws

The tax laws impacting the e-commerce sector in India can be segregated into three categories - *Income Tax Act, 1961 (ITA), Finance Act, 2016 and Central Goods and Services Tax Act, 2017 (CGST)*. The ITA has recently introduced a withholding tax obligation on e-commerce operators, and separately withholding and collection obligations on all buyers and sellers of goods irrespective of the medium. Further, to specifically target the non-resident e-commerce operators, which do not have any physical presence in India, the Finance Act, 2016 (amended in 2020) provides for charge of an equalisation levy. The CGST also contains a tax collection-at-source provision for the e-commerce operators.

Foreign Direct Investment

The *Foreign Exchange Management (Non-Debt Instruments)* Rules, 2019 (Non-Debt Rules) place several restrictions on e-commerce entities who have received foreign direct investment (FDI), and who participate in the 'marketplace' model, or where they act as a '*facilitator between buyer and seller*'. While 100% FDI is permitted in companies engaged in B2B models of e-commerce, FDI in the B2C segment is permitted only

[11]Sensitive personal data or information consists of the following categories of personal information that can identify a natural person: password; financial information such as bank account number or credit/debit card number or other payment details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information.

[12]While the Privacy Rules regulate the processing of sensitive personal data by non-Government persons, the Proposed Law may impose compliance requirements and relevant liabilities on Government entities as well (however, likely with significant exceptions regarding Government-related data processing).

[13]Ranjan Mishra, A. (2021, 23 July). *National e-commerce policy undergoing inter-ministerial consultation*. Livemint.https://www.livemint.com/news/india/national-e-commerce-policy-undergoing-inter-ministerial-consultation-11627041214284.html

in the marketplace model of e-commerce if certain conditions are met. The Non-Debt Rules do not permit FDI in the inventory model of e-commerce. Further, 100% FDI is permitted under automatic route for single brand retail trading but with certain conditions.

Legal Metrology

The *Legal Metrology Act, 2009* read with the *Legal Metrology (Packaged Commodities) Rules, 2011* prescribe compliance requirements for sellers on e-commerce websites, and require entities engaged in the marketplace model to ensure that the sellers comply with their mandatory disclosures.

Advertising Guidelines

The Advertising Standards Council of India, a self-regulatory voluntary organisation of the advertising industry, maintains the Code for Self-Regulation in Advertising which is applicable to the online medium. This Code contains guidelines for advertisements of specific goods and services, and prescribes for declaimers in certain instances. In addition, the Consumer Protection Act, 2019 prohibits 'misleading advertisements'. ASCI has also issued guidelines on *Advertising by Social Media Influencers which are in force*.

Competition Law

The *Competition Act, 2002* prohibits anti-competitive agreements, abuse of dominance and combinations that cause appreciable adverse effect on competition in India, which is regulated by the Competition Commission of India (CCI). The CCI has been relatively active in the e-commerce sector, and ordered investigations into the practices by leading e-commerce entities. In 2020, the CCI also released a 'Market Study on E-commerce in India'[14], which focused on the key trends and features of e-commerce, the competition issues in the industry, and the observations of the CCI based on these findings.

E-Contracts

E-commerce entities for the most part, conduct their sales, and hence enter into e-contracts and the IT Act provides validity to contracts formed through electronic means, with specific exemptions.

IP Protection

E-commerce entities should be vigilant about protecting their intellectual property, which includes the software in their platforms, trademarks and brand names, domain names and any artistic, musical or literary works to name a few.

[14]Competition Commission of India. (2020). *Market Study on e-Commerce in India: Key Findings and Observations*.https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf

04. Assessing Legal Obligations on Different Business Models within E-commerce

As captured in the '*Key Regulations Impacting E-Commerce*' chapter above, there are a plethora of laws that are applicable to the e-commerce sector irrespective of the specific business model. These include payment laws, data protection regulations, advertising guidelines, contract, and intellectual property considerations to name a few which apply across the board to all forms of entities that provide digital services. However, there are certain laws that apply only to certain business models in the e-commerce sector. We have identified these laws in the table below, where you may see our indicative analysis of the laws that may apply to the B2B, B2C and C2C platforms, as well as comments on possible over-regulation of the sector.

Regulation of Business Models	Consumer Protection Laws	FDI Restrictions	Legal Metrology	Intermediary Guidelines	Withholding under Section 194-O
B2B	✗	✗	✗	✓ (Only for marketplace model)	✓
B2C	✓	✓	✓	✓ (Only for marketplace model)	✓
C2C **Platform enabling C2C transactions**	✗ (The law is vague on this point as there is a possibility of regular sellers (beyond product sellers) also registering on platforms)	✗	✓	✓ (Only for marketplace model)	✓
Policy Intent	The policy intent is to ensure that consumer facing businesses implement measures for consumer protection and ensure that there is transparency, disclosures are made, and provide for grievance redressal.	The policy intended to control foreign investment especially in the multi brand retail trading sector.	Similar to the Consumer Protection law, the policy intent is to safeguard the interests of the consumer.		The policy intent is to ensure that the sellers are discharging income taxes and GST without evasion.
Analysis - Cases of Over Regulation	Due to the wide definition of e-commerce, the E-commerce Rules impose compliance obligations without regard to unique models and *inter se* relationships between the entities, buyers and sellers.	The condition of entities engaged in Single Brand Retail Trading to have physical stores is onerous. Further, the broad definition of marketplace entities leads to conditionalities on all forms of e-commerce entities who fall under the definition.	We see overregulation in this sphere vis-a-vis the compliance requirements vis-a-vis the marketplace.		Levying TDS on e-commerce entities without clearly defining the scope makes the case of over-regulation. The definition of e-commerce under section 194-O covers even those considerations which do not flow through the e-commerce plat-

Analysis - Cases of Over Regulation	Further, the obligations on mar ketplace entities, insofar as disclosures to be made are concerned, are onerous for entities who follow a 'hands off' approach, and those that are not involved in every aspect of the transaction and commerce value chain.				form. It is important that the regulations consider the practical challenges faced by the different business models in terms of their functionality. Certain business face impossibility to comply with the provisions.

05. Regulatory Framework around the World

5.1. OECD Recommendations

In 2016, the Organisation for Economic Co-operation and Development (OECD) released recommendations on 'Consumer Protection in E-Commerce' which recommended that both members[15] and non-members adhering to the recommendation work to implement specific principles in their policy frameworks. The OECD Recommendations define e-commerce as "*business-to-consumer e-commerce,*[16] *including commercial practices through which businesses enable and facilitate consumer-to-consumer transactions", that covers "commercial practices related to both monetary and nonmonetary transactions for goods and services, which include digital content products*." While India is not a full time member of the OECD, they are part of the OECD Development Centre. Highlights of these recommendations are as below:

01 Consumers should be afforded **transparent and effective consumer protection** that is not less than the level of protection afforded in other forms of commerce.

02 Businesses should act in accordance with **fair business, advertising and marketing practices** as well as the general principle of good faith.

03 **Online disclosures** on e-commerce sites should be **clear, accurate, easily accessible** and conspicuous, and in plain and **easy to understand** language.

04 The development of **internal complaints handling mechanisms by businesses**, which enable consumers to informally resolve their complaints directly with businesses, as well as the **formal dispute resolution process** should be communicated to the consumer.

05 Governments and stakeholders should work together to educate consumers, government officials and businesses about e-commerce to foster informed decision making.

06 Businesses engaged in e-commerce with consumers should:

(i) Make **readily available information about themselves** that is sufficient to allow, at a minimum: i) **identification** of the business; ii) prompt, easy and effective **consumer communication** with the business; iii) appropriate and **effective resolution of any disputes** that may arise; iv) service of **legal process** in domestic and cross-border disputes; and v) location of the business.

[15]Organisation for Economic Co-operation and Development. (2016). *Consumer Protection in E-commerce: OECD Recommendation*. https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdF

[16]The OECD Principles also include the: **Implementation Principles**: To achieve the General Recommendations above, Governments should work in cooperation with stakeholders towards improving the evidence base for e-commerce policy making, review and adapt laws protecting consumers in e-commerce, having in mind the principle of technology neutrality, establish and maintain consumer protection enforcement authorities, and encourage the continued development of effective co-regulatory and self-regulatory mechanisms; and the **Global Cooperation Principles**: Governments should facilitate communication, co-operation, and, where appropriate, the development and enforcement of joint initiatives at the international level among governments and stakeholders. The cooperation and coordination of local consumer protection authorities should also be encouraged, through existing international networks and enter into bilateral and/or multilateral agreements or other arrangements as appropriate.

(ii) Provide **information describing the goods and/or services** offered, and the **terms, conditions and costs associated** with a transaction that is sufficient to enable consumers to make **informed decisions** regarding a transaction.

(iii) Ensure that the point at which consumers are asked to **confirm a transaction**, after which time payment is due or they are otherwise contractually bound, is **clear and unambiguous**.

(iv) Provide consumers with **easy-to-use payment mechanisms and implement security measures** that commensurate with payment-related risks, including those resulting from unauthorised access or use of personal data, fraud and identity theft.

(v) **Provide redress** to consumers for the harm that they suffer as a consequence of goods or services; and **protect consumer privacy**.

The E-Commerce Rules in India seem aligned with these OECD principles, in so much as they bring in requirements for the disclosures to be displayed to consumers, as well as the institution of consumer grievance redressal mechanisms.

5.2. European Union

The E-Commerce Directive (**ECD**) issued by the European Union (EU) in 2000 contains guidelines for the e-commerce industry. The ECD governs the offering of "information society services", that were earlier defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".[17] The ECD focused on removing obstacles to cross-border online trade in the EU, as well as providing transparency and certainty to businesses and citizens. The ECD sets out basic requirements on mandatory consumer information, steps to follow in online contracting and rules on commercial communications. The ECD also exempts intermediaries from liability for the content they manage if they fulfil certain conditions. The liability exemption only covers services who play a neutral, merely technical and passive role towards the hosted content. Further, service providers hosting illegal content need to remove it or disable access to it as fast as possible once they are aware of the illegal nature of it. Further, the EU has released a Digital Single Market Strategy to introduce measures to remove barriers of entry for the e-commerce industry and ensure better access for consumers to goods across Europe.[18]

The Fairness and Transparency of Online Platform Regulation issued in 2019 imposes new rules on intermediaries (including e-commerce platforms).[19] Article 5 in particular lays down the requirement that platforms must be transparent about how their search engines work.[20] When an intermediary search engine produces a set of ranked results, it must be able to justify the results, since the ranking of products on an e-commerce platform is strongly correlated with the likelihood that the product will be seen and purchased by a consumer. Intermediaries must also be transparent about policies pertaining to the product reviews and ratings

[17]'Information society services': services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC.

[18]Brotman, S. N. (2016). The European Union's Digital Single Market Strategy: A conflict between government's desire for certainty and rapid marketplace innovation. Center for Technology Innovation at Brookings

[19]Rüffer, I., Nobrega, C., Schulte-Nölke, H., & Wiewórowska-Domagalska, A. (2020). The legal framework for e-commerce in the Internal Market. Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652707/IPOL_STU(2020)652707_EN.pdf.

[20]Voigt, P., Reuter, W. (2019, September 13). Regulation on promoting fairness and transparency for business users of online intermediation services (P2B-Regulation). TaylorWessing. https://www.taylorwessing.com/en/insights-and-events/insights/2019/09/verordnung-zur-frderung-von-fairness-undtransparenz-fr-gewerbliche-nutzer-von-onlinevermittlungsdie

– these tend to play a large part in influencing sales and influence the ranking of products. The regulation requires that intermediaries must state if the rankings can be altered in exchange for 'direct or indirect remuneration'.[21] They are exempt however from providing those details that might lead to manipulation of their algorithms or that violate their copyrights.

5.3. USA

E-commerce businesses in the US are treated on the same pedestal as the traditional retail business.[22] However, owing to the federal structure of the country, each state has their own laws which e-commerce entities operating in these states will need to keep in mind. Applicable to both offline and online commerce, the Magnuson-Moss Warranty Act ("**MMWA**")[23] is a central law governing consumer product warranties. The MMWA mandates written warranties on consumer products costing more than USD 10, along with requirements for warrantors or sellers to comply with.[24] Further, the Federal Trade Commission's ("**FTC**") guidelines on advertising apply to electronic marketing as well. It derives its authority from Section 5(a) of the Federal Trade Commission Act that prohibits "*unfair or deceptive acts or practices in or af ecting commerce*", be it on any medium.[25] The FTC Guidelines put the onus on sellers to be responsible for the claims they make about their products/services, as well as bringing in third parties within the ambit of the law where they also might be held liable for disseminating deceptive representations. Further, if a business uses emails for commercial purposes, the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003, ("**CAN-SPAM Act**"), becomes a critical law to comply with. Some of the main requirements under the-CAN-SPAM Act is informing the recipient where one is located, avoiding the usage of false/deceptive subject line and header information, honouring opt-out requests among others. The CAN-SPAM Act excludes transactional/relationship content from its ambit.[26]

5.4. United Kingdom

Similar to most jurisdictions, the UK does not have an overarching legislative or regulatory framework in the realm of e-commerce. Rather, there exist several legislations and regulations that specifically address the various aspects of e-commerce.

The liability scheme for online platforms in the UK is based on the European Union's ECD, under which platforms are protected from liability for any illegal content they host (rather than create), provided they take it down as soon as it is brought to their attention. Also based on the ECD, the E-Commerce Regulations, 2002[27] also provide for the mandatory disclosure of certain information[28] to consumers, which must be done at the pre-contract stage itself. Interestingly, while the E-Commerce Regulations apply to B2B and B2C businesses, B2B businesses can exercise the option to contract out of most requirements under the Regulation. E-commerce businesses that are engaged in the provision of services must also comply with the

[21] *Id*.

[22] Gill, J., Timon, V. (2021). USA: Digital Business Laws and Regulations, 2021. ICLG. https://iclg.com/practice-areas/digital-business-laws-and-regulations/usa

[23] 15 USC §§ 2301-2312.

[24] The Disclosure Rule, 16 C.F.R. Part 701; The Pre-Sale Availability Rule 16 C.F. R. Part 702

[25] Federal Trade Commission. (2000). Advertising and Marketing on the Internet. https://www.ftc.gov/system/files/documents/plain-language/bus28-advertising-and-marketing-internet-rules-road2018.pdf.

[26] Federal Trade Commission. (2009, September). CAN-SPAM Act. https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

requirements of the Provision of Service Regulations, 2009[29], and are subject to the Consumer Contracts Regulations, 2013 and the Consumer Rights Act, 2015.[30]

A recent Online Harms Whitepaper issued by the British government lays out many potential harms in the domain of e-commerce.[31] In *Tamiz v. Google Inc.*, Google was held liable for failing to remove defamatory material even after being notified of it.[32] We have already seen this model employed by the EU, the US and Canada.

5.5. Australia

In Australia, much of the conversation surrounding e-commerce regulation and disputes pertains to digital news media. In 2018, the Australian Competition and Consumer Commission (**ACCC**) found a growing imbalance of power between social media companies and news companies.[33] To combat the issue, the government issued the Digital Platforms Inquiry Final Report in 2019.[34] Several recommendations were made: (i) inquiry into ad tech services, (ii) code of conduct for negotiations between platforms and media businesses, including commitments related to data sharing and product ranking and (iii) prohibition on unfair trade practices. The ACCC also launched a Digital Platform Services Inquiry in July 2021 into potential competition and consumer issues in the provision of general online retail marketplaces to consumers in Australia. The ACCC sought views from stakeholders on these issues and seeks to submit a report with their findings.[35]

Similar to other jurisdictions, Australia also does not possess a single, unified legislative to regulatory framework to govern e-commerce entities. The primary legislative instrument for Consumer Protection in Australia is Schedule 2 to the Competition and Consumer Act, 2010, which is also known as the Australian Consumer Law (**ACL**). The ACL provides for a list of mandatory requirements that must be followed by all businesses, including e-commerce businesses.[36] Parties cannot contract out of their prescribed obligations under the ACL. Australia has also published guidelines to promote e-commerce and boost consumer confidence in

---

[27]The Electronic Commerce (EC Directive) Regulations. (2002). https://www.legislation.gov.uk/uksi/2002/2013/contents/made

[28]The minimum details that are required to be disclosed are as follows: Trader Name; Trader's Address; Trader's Email Address; Registration Number; VAT Number (If deemed applicable); and Details of any Supervisory Authority (If the entity is under a supervisory scheme).

[29]An Ecommerce Business engaged in the provision of services must provide sufficient details on the following:Main Features of the Services Provided; Any Multi-Disciplinary Services; Any Non-Judicial Dispute Resolution Measures that the Seller might be using; General Terms & Conditions in use; Contact Details for Requesting Further Information or Filing a Complaint

[30]Under the Consumer Contracts Regulations, an E-commerce business must provide information regarding Main Characteristics of Goods, Services or Digital Content Provided; Total Price or Manner of Price Calculation; Accepted Means of Payment; Delivery Restrictions or Additional Delivery Charges; Costs Imposed on a Periodic Basis in case the contracts provides for it. Under the Consumer Rights Act, an E-Commerce Business must also provide the consumer with the right to cancel an online contract and receive a refund within a prescribed cooling-off period of 14 days. Further, the Act provides that any right of cancellation or any applicable conditions must be duly communicated to the consumers.

[31]Department for Digital, Culture, Media & Sport. (2020). *Online Harms White Paper.* https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper#a-new-regulatory-framework

[32]Bristows LLP. (2019, August 15). *E-Commerce in United Kingdom*. https://www.lexology.com/library/detail.aspx?g=dea011e4-dde0-41e4-a18a-78f52199a8c5

[33]Deam, BBC. (2021, February 18). *Australia news code: What's this row with Facebook and Google all about?* BBC. https://www.bbc.com/news/world-australia-56107028

[34]4 Australian Competition & Consumer Commission. (2019). *Digital Platforms Inquiry - Final Report.* https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

[35]Digital Platform Services Inquiry – March 2022 Report on general online retail marketplaces (Issues Paper).(2021). https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry%20-%20March%202022%20report%20-%20Issues%20paper.pdf

[36]Competition and Consumer Act, 2010 (Australia), Schedule 2. https://www.legislation.gov.au/Details/C2017C00369

this space. The Australian Guidelines for Electronic Commerce,[37] published in consultation with the Commonwealth Consumer Affairs Advisory Council (CCAAC) contains a list of guidelines and best practices to be followed.[38]

While there doesn't appear to be a uniform approach towards the governance of e-commerce platforms in these jurisdictions, a common thread is the mandate of appropriate disclosures to be given to consumers among other requirements for consumer protection that the OECD principles in 2016 had recommended. The E-Commerce Rules of India notified in 2020 follow this global trend with regard to the requirement of disclosures to consumers.

[37]The Australian Guidelines for Electronic Commerce, 2006 (Australia). https://treasury.gov.au/sites/default/files/2019-03/australian_guidelines_for_electronic_commerce.pdf

[38]These best practices include: 1. Fairness in Business Practices 2. Accessibility for Users 3. Accessibility for Users with Disabilities 4. Advertising and Marketing Practices 5. Best Practices for Engagement with Minors 6. Disclosure of Information Pertaining to Identification of the Business 7. Disclosure of Information Pertaining to Contractual Matters 8. Conclusion and Performance of Contracts 9. Privacy 10. Payment Related 11. Security and Authentication 12. External Dispute Resolution 13. Applicable Law and Fora of Dispute Resolution 14. Internal Complaint Handling Procedures

06. Key Policy Challenges

Policymaking in e-commerce should aim at enabling innovations - both in technology and in business models, encouraging the barrierless entry of start-ups, investments, infrastructure growth, building consumer trust, fair competition and employment generation. The focus should be accelerating growth rather than imposing unnecessary controls. The policy should be inclusive where Central and the State governments work hand in hand.

Before we delve into specific suggestions, we have discussed a few overall principles that we recommend be considered by regulators in the e-commerce space:

First, any regulatory design must be in principle focused on addressing specific mischiefs and concerns rather than create all pervasive rules. The policy should be based on empirical data rather than perceived harms.

Second, laws addressing online businesses separately from offline businesses should be limited to the extent of addressing the change in medium. However, existing regulation imposes differential treatment on e-commerce marketplaces: as an example, the law does not expect an offline marketplace to be accountable in any manner for the acts of its sellers. Under Article 14 of the Constitution, intelligible differentia is an essential prerequisite for a law to be constitutional. When a provision, whose objective would extend to both online and offline stores, is imposed only on e-commerce platforms, the criteria of intelligible differentia is not fulfilled. Hence, e-commerce regulation should account for this constitutional prerequisite in its design and avoid the selective imposition of commerce-related obligations only on the e-commerce sector in disregard of similar activities taking place offline.

Third, laws should take into account the fact that business models will keep innovating and evolving, and that such innovation should be encouraged. The e-commerce ecosystem is large and diverse enough that a one-size-fits-all policy no longer ascribes to the current ecosystem.

Fourth, consumer protection should be at the core of the policy decisions. Currently, in online market places, this reluctance stems from the perceived and occasionally real risk imposed by buying from unknown vendors and suppliers. Common concerns among consumers include data privacy and security[39] (including fears about fraud and identity theft), product quality, uncertain delivery, scope of replacement, and many others.[40] Consumers are more likely to trust e-commerce entities if they are confident that an error can be corrected with swift and reliable redressal. The Consumer Protection (E-Commerce) Rules, 2020 make great strides in this regard, by providing for a mandatory grievance redressal mechanism.[41] If functional and enforced effectively, grievance redressal can have an enormous impact on consumer trust.

Consumers are also less likely to be anxious about seller reliability if the entire process, from purchase to delivery to replacement to grievance redressal, is legible.[42]

---

[39]Raghavan, K., Desai, M.S., & Rajkumar, P.V. (2017). *Managing Cybersecurity and e-Commerce Risks in Small Businesses*. Journal of Management Science and Business Intelligence, 2(1), 9-15. http://ibii-us.org/Journals/JMSBI/V2N1/Publish/V2N1_2.pdf

[40]Chawla, N., & Kumar, B. (2021). *E-Commerce and Consumer Protection in India*: The Emerging Trend. Journal of Business Ethics. Journal of Business Ethics. https://doi.org/10.1007/s10551-021-04884-3

[41]Section 5(5), Consumer Protection (E-Commerce) Rules, 2020

[42]Brendon, C.F. (2002). *In ecommerce, customer trust is no longer an option: It is the requirement for success*. International Quality Management Pty Ltd. https://www.proquest.com/openview/ae1d8048a54b71570f7d10ddbe5b1f62/1?pq-origsite=gscholar&cbl=39817

At the same time, when a consumer wishes to take a risk, the regulations should not scuttle the transactions. E.g. in a C2C e-commerce, the consumer is generally aware that they may not have a remedy against the seller. The consumer is willing to take that risk due to the lower price. In such a case, generating consumer awareness may be a way forward rather than scuttling C2C business models.

E-commerce businesses face a heavily competitive market while being required to comply with an ambiguous regulatory scheme and a demanding compliance regime. Some of the policy challenges for businesses include:

6.1. Overbroad Definition of E-commerce

The E-commerce Rules, 2020 do not accommodate the differences between various e-commerce models and use an overbroad definition to impose obligations on entities which may not even operate a marketplace, such as tech companies, which do not play any other role besides providing the platform.

The proposed amendments define an e-commerce entity to *include 'any entity engaged … for the purpose of fulfilment of orders*.' The proposed amendment may be interpreted to include ancillary partners of e-commerce entities, such as those providing cloud services, SaaS, or any other fulfilment service. It is important to note that several fulfilment partners often do not own, operate or manage a digital or electronic facility or platform. Compliance obligations for fulfilment partners and ancillary services must be distinct from those of e-commerce entities in accordance with the difference in functionality.

An overbroad definition will result in significantly increasing the compliance burden across the sector and cover services which may not be intended by the regulation. A prime example of this could be the equalisation levy 2020 for which the Finance Minister had to specifically exclude e-trade of rough diamonds from its ambit.[43] This may happen to several other industries who might get covered due to these overbroad definitions. Additionally, several SMEs that provide ancillary services will be discouraged from engaging with e-commerce because the cost of entry in the market is too high. This only increases the ambiguity within the sector and risks overlapping regulations, which inevitably increase the compliance burden.

6.2. Overregulation and a one-size-fits-all approach

The earlier chapters have covered the regulations that apply to e-commerce entities and it must also be kept in mind that the entities have to observe sector specific laws. For example, cab aggregators would have to comply with Motor Vehicle Act, 1988 and entities in the payment space have to comply with a number of guidelines issued by the RBI. Currently, the one size fits all approach in terms of both revenue generated and business models, has significantly affected the ecosystem. The overregulation and increased compliance burden may create entry barriers for the new entities willing to compete in the market. For example, as observed earlier, proposed amendments to e-commerce rules approach the e-commerce ecosystem with a one-size-fits-all policy, which if implemented, could have a devastating effect for new entrants in the market or small existing companies. Further, reduced compliances also encourage innovation and growth in a sector. Case in point could be the Drone Rules 2021, which has made significant strides in easing the compliance burden and encouraging innovation while ensuring the security which has been welcomed by the industry.

[43]TNN. (2020, August 28). *FM's clarification* on EL a big relief for diamond industry. The Times of India. https://timesofindia.indiatimes.com/city/surat/fms-clarification-on-el-a-big-relief-for-diamond-industry/articleshow/77790794.cms

Several obligations under the E-Commerce Rules and the Proposed Amendments appear to have been drafted with the intention of imposing obligations on 'hands on' e-commerce entities. These include e-commerce entities that are involved in every aspect of the transaction and commerce value chain between buyers and sellers, i.e., those entities involved in order placement, confirmation and fulfilment, logistics, delivery, etc. On the other hand, "Hands off" marketplace e-commerce entities that function as intermediaries and simply provide a platform for search and discovery of goods and not for actual sale and purchase transactions (similar to that of enabling an online window shopping but not actual sales), should not be burdened with heavy obligations. It needs to be kept in mind that newer platforms could undertake more singular functions such as enabling discovery of buyers and sellers on its platform or undertake significantly lesser functions compared to traditional marketplaces by being a mere intermediary. However, the original rules as well as the proposed amendments appear to impose the same level of compliance obligations and accountability on all platforms, without taking into consideration the variances in operational models.

There should be an express exemption/carveout from these obligations for such "hands off" marketplace e-commerce entities. Further, any obligation imposed on "hands-off" marketplaces should be proportionate to the functions they carry out on a model to model basis only. Onerous obligations without being cognisant of the dynamism of various platforms involved in the e-commerce value chain might have a negative effect on its growth in India, which would ultimately adversely affect the consumer.

Further, complying with different kinds of law, even though it may or may not have relevance to the business, is cost defective as well as increases the burden on the entities. For example - marketplace entities have the requirement of publishing the country of origin even though it is not selling the product directly and that increases their burden. Similarly, the collection of TDS for the purpose of recording transactions also seems unnecessary when it could be solved from a simple reporting requirement. It further creates friction between different laws and results in forum shopping. For example, Rule 5, clause 14 (a) of the proposed amendments venture into aspects of data sharing and processing (based on consent), whose nuances can best be dealt with a Data Protection Authority (DPA), and overarching Data Protection law. Further, the overlap with competition law also brings the CPA in conflict with that of CCI, possibly contributing to more 'forum shopping' and delaying strategies. With e-commerce policy also in the pipeline, there is a possibility of creation of an e-commerce regulator which will again come in conflict with the existing regulators.

6.3. Intermediary Rules

The section 79(1) of the IT Act provides that, subject to a few prerequisites, intermediaries will not be liable for any third-party information posted by them. This creates a safe harbour regime for intermediaries undertaking the due diligence requirements provided in intermediary guidelines. Section 2(w) of the IT Act includes online marketplace within the definition of 'intermediary'. Through multiple judgments[44], Indian forums have clarified the applicability of intermediary liability provisions on e-commerce platforms.

However, the advent of the E-Commerce Rules, 2020 presents a new conundrum. E-commerce entities also have to comply with the provisions of the Consumer Protection Act, 2019 in order to avail this safe harbour provision. The additional mandate to comply with the Consumer Protection Act, 2019 creates new liabilities and provides little to no clarity on the penalty that may be imposed in cases of violation. On the other hand, Rule 5 of the Rules allow a marketplace e-commerce entity to avail the safe harbour provision[45] if it also complies with Sections 79(2) and (3) of the IT Act. The E-commerce Rules, 2020 provide that in case of any violation of the E-commerce Rules, 2020, the provisions of the Consumer Protection Act, 2019 will apply.

[44]See Kent Ro Systems Ltd & Anr v Amit Kotak & Ors, 2017 (69) PTC 551 (Del); Amazon Seller Services Pvt Ltd v Modicare Ltd, FAO(OS) 133/2019.

[45]Section 79, Information Technology Act, 2000.

6.4. Proposed amendments to the Consumer Protection (E-commerce) Rules

The proposed amendments to the Consumer Protection rules puts onerous burdens on e-commerce entities and transgress into the domain of other regulators. Following are the some of the issues arising out of the proposed amendments:

6.4.1 Increased compliance burden

The proposed amendments add compliance obligations such as requiring e-commerce entities to register in India, present domestic alternatives to goods on their platforms, and list countries of origin. Offline vendors of the same products do not have to comply with this requirement. In accordance with Article 14 of the Constitution, which lays down the principle of intelligible differentia, online vendors can have varied compliance measures *only* to the extent required to address the change in medium. Additionally, the E-commerce Rules, 2020 also requires that entities have justifiable grounds for price changes of goods.[46] These are sweeping changes that may have the capability to disrupt market dynamics, as well as long standing parts of the business strategies and models of e-commerce companies.

Small and domestic e-commerce businesses are likely to be disproportionately affected by the proposed amendments. Clause 4 of the proposed amendments requires every e-commerce entity to register with the Department for Promotion of Industry and Internal Trade (DPIIT) and display their registration on their website. Clause 5(b) requires even start-up e-commerce companies (which usually have a few employees), to have a 24x7 employee. The proposed amendments also creates fallback liability for the e-commerce entity when a seller fails to deliver goods in contravention of the e-commerce entity's prescribed process.[47] The 2020 Rules also impose entity localisation obligations, which may be an unreasonable requirement since there are legal and technical solutions available under the IT Act to enforce Indian laws against an entity with digital presence. Taken together, they represent a significant increase in compliance burdens that are starkly at odds with the government's goals of improving India's ease of doing business ranking and encouraging entrepreneurship.

6.4.2. Unreasonable Trade Restrictions

Suppose a brand decides to launch its own website but does not want to deal with B2C sales directly. It would onboard its distributors onto the website as sellers. However, this arrangement would be prohibited under the proposed amendments, since a marketplace entity cannot do B2B transactions with sellers on its own website. It also cannot use the marketplace brand to promote goods sold on a website. This is an unreasonable trade restriction on the business arrangement of a particular entity and beyond the scope of the CPA itself.

Another such restriction is on associated enterprises and related party sellers, who are not allowed to sell on the marketplace. If a group of companies create a single entity to manage a website, the proposed amendments prevent the companies from selling on this website due to the restriction on related party sellers. For example, if an investment entity invests in SMEs and these SMEs try to access a particular marketplace, they would be disallowed if the investment entity and marketplace entity are associated enterprises. This leads to a situation where the SMEs have to choose between investment and access to a marketplace.

[46]Section 5(14)(a), Consumer Protection (E-Commerce) Rules, 2020.

[47]Section 6(9), Consumer Protection (E-Commerce) Rules, 2020.

6.4.3. Overlap with Existing Laws

The proposed amendments also deal with competition law, despite the presence of a separate legislation and regulator for competition issues, and the regulator is already looking into e-commerce marketplaces. Further, the Rules presume that certain arrangements are anti-competitive without any scope for rebuttal, thereby going against the construct of the Competition Act, 2002. The Rules also overlap with the mandate of the proposed Data Protection Bill through its provisions on data, existing GST invoicing rules through its provisions on marketplace invoicing, and existing legal metrology legislation that obligates the "country of origin" tag on a marketplace. This overlap not only creates confusion with respect to the other legislation, but goes beyond the scope of the parent legislation CPA since it is not limited to the scope of consumer interest.

6.5. FDI Policy

The present FDI Policy poses several challenges for e-commerce growth. Several aspects of the policy need to be revisited in order to secure further FDI for growth of the e-commerce sector (and the economy) and ensure the consumer's right to access a variety of goods and services. These issues are highlighted below:

6.5.1. Sale of Third-Party Sourced Goods

A manufacturing company having FDI is not allowed to sell third-party sourced/imported goods on a B2C basis on its platform where it is allowed to sell its own manufactured goods. This restriction fails to account for the fact that the manufacturing company is already contributing to the Indian economy and thus should be allowed to sell third-party sourced /imported goods to some extent, at least in the same or related category as the manufactured goods.

6.5.2. Marketplace for Services

There are certain conditions on marketplaces that arise from the policy that 100% FDI is not permitted in multi brand retail trading (**MBRT**) in goods. Certain conditions are also imposed on marketplaces for services. These conditions prevent LLPs who operate such marketplaces from attracting FDI. However, since FDI is 100% permissible in e-commerce services, there should be no conditions attached to the marketplaces for such services.

6.5.3. Single Brand Retail Trading

Entities who are entitled to 100% FDI under automatic route for single brand retail trading (**SBRT**) cannot operate e-commerce platforms unless they have physical stores. Such an SBRT entity would contribute to the economy through employment and logistics through operation of an e-commerce platform, even if it does not have a physical store. This condition of requiring physical stores need to be removed keeping in mind that the offline and online market should be considered a single market. Other aspects related to SBRT entities need to be simplified. Firstly, it might be clarified that sub-brands sold under a single brand would still amount to SBRT. Secondly, the condition that Indian brands should be owned and controlled by Indian entities must be removed in order to give impetus to brands originating in India and to prevent unnecessary confusion for FDI. Lastly, the sourcing norms for SBRT entities need to be simplified such that the entity has an option to contribute to the Indian economy through various routes in addition to sourcing. For example, through additional CSR spends.

6.5.4. Multi Brand Retail Trading

MBRT entities with FDI should be B2C e-commerce, subject to certain conditions that should be left to states and union territories to decide.

6.5.5. Definition of Marketplace

There are several Indians start-ups which provide tech platforms for SMEs to get online. These start-ups do not provide any other services, except payment integration to such sellers. If an FDI investor were to invest in such a start-up, and also invest in other SBRT entities, the FDI policy would prevent the other entities from availing the platform of the start-up. This leads to a situation where the investor has to choose between the 'marketplace' start up and the seller entities. Given their limited role in providing a platform and nothing beyond, such entities should not be considered marketplace entities under the FDI policies in order to prevent such situations.

6.6. Taxation

The current tax regime in India places significant compliance burdens on the e-commerce entities. There are multiple withholding and tax collection obligations on e-commerce operators, which generally overlap with each other. From a tax policy perspective, the provisions fail to take into account different e-commerce models and treat all of them alike, without considering the commercial reality. For example, withholding tax under section 194-O requires the e-commerce operator to deduct tax on payment to the e-commerce participants even when the consideration does not pass through them, which seems quite impractical (as compared to TCS under GST which does not apply unless consideration is collected by the platform). Further, disparity between offline and online sellers in terms of registration thresholds and availing the composite scheme under GST by sellers on e-commerce platforms, creates a bias against online sellers.

	Section 194Q	**Section 1940**	**Section 206C(1H)**	**Section 206C(1H)**
Applicability	Purchase of goods of value exceeding INR 50 lakhs	Sale of goods or provision of services through a digital platform	Sale of goods of value exceeding INR 50 lakhs	Sale of goods or provision of services through a digital platform
Obligation On	Buyer responsible for paying any sum to resident	Ecommerce Operator (Even if payment is made by a purchaser directly to the e commerce participant)	Seller	Ecommerce Operator (only if consideration flows through such operator)
Time of deduction/ collection	Credit of sum to the account of the seller or at the time of payment thereof by any mode, whichever is earlier	Credit of amount to account of an e-commerce participant or at the time of payment thereof to such e-commerce participant by any mode, whichever is earlier	Receipt of consideration from buyer	In the month in which supply has been made through the platform
Rate	0.1% on amount exceeding INR 50 lakhs	1%	0.1% on amount exceeding INR 50 lakhs	1% on net value of taxable supplies

Fig 4: Snapshot for tax compliance provisions

The intent behind different withholding/collection provisions, seems to *widen and deepen the tax base*[48], and given the low rates of taxes (0.1% - 1%), they may not be a mechanism for tax collection per se, but an information collection tool to ensure wider compliance. The recent circular[49] clarifying the manner in which 194-O, 194Q and 206C are interlinked and the instruction that if one is complied with, then the other withholding obligations do not apply clearly suggest that the policy goals are similar.

The Central Board of Direct Taxes and Central Board of Indirect Taxes and Customs already have a Memorandum of Understanding[50] for data sharing between both the organisations. Hence, information collected under TDS provision[51] of the ITA concerning e-commerce suppliers, may be easily accessible through information submitted under GST return.[52]

In case the consideration does not flow through an e-commerce platform, it should not be considered in scope for the withholding tax base. The withholding/collection provisions under ITA and CGST may become a major problem for the entities who sell their product in large volumes with low margins, as although the credit of the taxes paid accumulate, obtaining refunds is a cumbersome process which affects the working capital requirements. Further, there is a need for bringing parity between online and offline sellers. Currently, offline retailers get exemptions for registration under GST if their intra state sale is less than INR 40 lakhs (goods) and INR 20 Lakhs (services). Similarly, offline sellers also enjoy the benefits of composition schemes. However, any online seller would have to obtain mandatory registration even if they make a single sale online and also do not qualify for the benefits of the composition scheme as an online seller. Such a disparity creates a barrier for the sellers to shift to online marketplaces who will have to comply with these obligations and puts them at competitive disadvantage compared to offline retailers. Therefore, non-discriminatory treatment of online and offline sellers woul increase consumer benefits through increased competition across the market.

Additionally, where e-commerce marketplaces are subject to a 2% EL on the gross value, disproportionate obligations are cast upon the e-commerce entities as they may be required to be cognizant of the residential status and manner of access to the platform by their customers. Further, it might be impractical or unfeasible for e-commerce operators to keep track of the IP address or the location of each customer as tracking IP addresses may add to compliance cost.

Hence, as a guiding principle, the law should not impose impractical or impossible conditions for the taxpayers and should seek to apply provisions strictly tailored to their current business and operational model.

[48]Memorandum to Finance Bill, 2020

[49]Central Board of Direct Taxes. (2021, June 30). Guidelines under Section 194Q of the IT Act, 1961. Circular No. 13 of 2021. https://www.incometaxindia.gov.in/communications/circular/circular_13_2021.pdf

[50]Central Board of Direct Taxes. (2020, July 21). *Memorandum of Understanding (MoU) between CBDT and CBIC signed today* [Press Release]. https://www.incometaxindia.gov.in/Lists/Press%20Releases/Attachments/848/PressRelease_MoU_between_CBDT_and_CBIC_21_7_20.pdf

[51]Form No. 26Q, Income Tax Rules. https://www.incometaxindia.gov.in/forms/income-tax%20rules/103120000000007861.pdf

[52]Form GSTR - 8. https://www.webtel.in/Image/Form%20GSTR_8_New.pdf

6.7. Supply Chain Partners

The e-commerce model makes it difficult for companies to ensure that their supply chain partners are functioning in a sustainable, inclusive, and responsible manner. The National Guidelines on Responsible Business Conduct, 2019, provide that an entity should ensure that there are systems and processes in place to enable its value chain partners to comply with regulatory requirements pertaining to their employees. However, the guidelines do not explain the manner in which this can be ensured within the e-commerce ecosystem, where entities adopt a "hands off" approach. The platform rarely interferes in the relationship between manufacturers, suppliers and distributors. While ensuring suitable and sustainable supply chains is an important practice, the guidelines do not provide a practical working model within the e-commerce ecosystem.

6.8. Regulators

Regulation of e-commerce entities primarily takes place along two axes. First, sectoral regulators which regulate e-commerce entities as a matter of course (e.g., state transport authorities which regulate ride hailing and online booking apps). Second, umbrella regulators who seek to regulate across sectors (e.g., the proposed Data Protection Authority, the Competition Commission of India, etc.). This may lead to jurisdictional overlaps as delved into below:

E-commerce disputes can be contractual (e.g. B2B or B2C) or non-contractual (intellectual property,[53] data protection, competition law, etc.).[54] Non-contractual issues pose unique problems in India. The CCI, for instance, regularly tracks e-commerce entities for abuse of dominance and anti-competitive behaviour including actions related to search ranking, product pricing, and other issues. However, the CCI's role as an umbrella regulator presents jurisdictional issues in the presence of sector-specific laws, as discussed in *Competition Commission of India v. Bharti Airtel*.[55] The E-Commerce Rules, 2020 seek to govern certain subjects that have ordinarily been brought before the CCI, for instance, search rankings. Specifically demarcating the jurisdiction of multiple forums relevant to e-commerce is going to be a challenge and needs consideration.

Additionally, the sheer number of regulators rapidly increases the risk of jurisdictional conflicts, such as the conflict between the Telecom Regulatory Authority of India ('TRAI') and the CCI.[56] Currently, the laws of e-commerce are being administered by a host of regulators such as MeitY, DPIIT, CCI, CPA, RBI, Income Tax Department, Foods and Public Distribution. The scenario is expected to become more complicated once the Data Protection Bill is enacted. Clause 53 of the Data Protection Bill allows the Personal Data Protection Authority to conduct an inquiry into the manner personal data is processed by data fiduciaries. Tussles between competition law and data privacy are not uncommon. Further, civil forums have the jurisdiction to entertain other aspects of e-commerce, including taxation and intellectual property. Resolving these issues would be crucial to provide transparency to e-commerce entities regarding complaint mechanisms.

[53]Velu, A.M. (2016). *IP Disputes in E-Commerce – A Jurisdictional Dilemma*. Altacit, Manupatra Intellectual Property Reports. https://www.altacit.com/ip-management/ip-disputes-in-e-commerce-a-jurisdictional-dilemma/

[54]Mishra, S. (2020). *Determining Jurisdiction over E-Commerce disputes in India*. Manupatra. http://docs.manupatra.in/newsline/articles/Upload/FE4BA350-DBEF-49DA-97D4-09E54ED8B813.pdf[50]Central Board of Direct Taxes. (2020, July 21). Memorandum of Understanding (MoU) between CBDT and CBIC signed today [Press Release].

[55]2019 2 SCC 521

[56]Philipose, M. (2018, 21 December). *Despite Supreme Court weighing in, TRAI-CCI friction looks far from over*. Livemint. https://www.livemint.com/Money/bzKy3cYolJmJlWGB3MM1hN/Opinion-Despite-SC-weighing-in-TraiCCI-friction-looks-far.html

The tendency to see e-commerce or internet business regulation as a monolithic category, instead of seeing a variety of sectors enabled by similar technology, creates a preference for umbrella regulators. Policymakers must overcome this pattern, and as long as we do have umbrella regulators, work to ensure clear delineations of authority, including MoUs and mandatory consultations between regulatory bodies. India has to move forward from the concept of legal pluralism in the e-commerce ecosystem if it intends to truly exploit the potential of e-commerce.

7. Way Forward

7.1. Provide for a clear definition of e-commerce and of 'inventory' and 'marketplace' entities

As previously discussed, there are overly broad and overlapping definitions of 'e-commerce' as well as of 'inventory' and 'marketplace' e-commerce entities in India. While providing very granular definitions may be challenging, considering the dynamic nature of the ecosystem, it is important to adopt measures to minimise ambiguity within the sector. An alternative, therefore, could be to expressly exclude entities, such as those that follow a hands-off approach or offer ancillary services, from the ambit of the E-Commerce Rules or seek guidance from internationally accepted definitions, such as the one in the OECD Guidelines.

7.2. Consider a light touch regulatory approach

The existing regulatory approach enforces the same mandates for e-commerce entities that vary in scale and in the services that they offer. In order to create a level playing field within this sector, it is important that entities are given differential treatment based on their size and functionality. For instance, entities that follow a 'hands off' approach or do not actually enable sales and simply provide an online catalogue and the like should be provided different treatment on the basis of their varied functionality. These onerous compliance burdens could hamper the growth of the sector and create entry barriers for the new participants.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 may distinguish between 'intermediaries' and "significant" social media intermediaries, and provide additional compliance obligations for the latter. Creating uniform mandates across the sector can lead to SMEs being disproportionately affected. Levying TDS from models that do not facilitate transactions is one such example. Operating with fewer resources, SMEs may struggle to comply with the rules and manage instances of proposed fall back liability. Therefore, a light touch regulation would eliminate the compliance burdens on the entities and would foster their growth.

7.3. Develop a co-regulatory approach

Regulators such as Telecom Regulatory Authority of India (TRAI), Competition Commission of India (CCI), Ministry of Electronics and Information Technology (MeitY), Department for Promotion of Industry and Internal Trade (DPIIT), and Consumer Protection Authority (CPA) govern different, and often overlapping aspects of e-commerce. This may also lead to regulatory arbitrage. It is important to consider a co-regulatory approach for governing these aspects of e-commerce. This would help the industry in giving their inputs and concern upon which the regulators can act.

7.4. Engage in participative and open consultative process

The e-commerce entities make up a large and diverse industry, with their own unique requirements and obligations. In order to create a dynamic policy that not only supports the consumer, but also encourag innovation and development within the market, it is important to engage in an open and consultative process for policy formulation. An important aspect of creating and maintaining a level playing field within the sector is that of creating a participative group of industry experts, companies, government officials, and other stakeholders. Consultations must be public in order to maintain transparency and accountability.

ANNEXURE – Key Regulations Impacting E-Commerce

A. Legal and Regulatory

(i) FDI Policy

The *Foreign Exchange Management (Non-Debt Instruments) Rules, 2019*, notified on October 17, 2019, incorporated the consolidated Foreign Direct Investment Policy, 2020 (**FDI Policy**) and was amended by the Ministry of Finance in 2020, and issued various Press Notes thereafter, as a consolidated regulation (**Non-Debt Rules**).

The Non-Debt Rules distinguish between two models of e-commerce. One is an "*Inventory model of e-commerce", where the "inventory of goods and services is owned by [the] e-commerce entity and sold to consumers directly*". The other is a "Marketplace model of e-commerce", where an e-commerce entity provides a digital platform and "*act[s] as a facilitator between buyer and seller*". While FDI in the inventory model is not permitted, the Non-Debt Rules prescribe the following important restrictions on the marketplace model:

- An entity that has received an investment from an "e-commerce marketplace entity" or its group companies is prohibited from selling its goods on an e-commerce platform run by the investor entity;[57]
- A marketplace shall not exercise ownership over the inventory, i.e. , goods purported to be sold.[58]
- An "e-commerce entity providing a marketplace" must offer services "at arm's length" and is prohibited from discriminating amongst vendors.[59]

Further, 100% FDI is permitted under automatic route for single brand retail trading (SBRT). However, such entities cannot operate e-commerce platforms unless they have or propose to have physical stores. FDI in SBRT is also subject to conditions such as: (i) products to be sold should be of a 'single brand' and the products should be sold under the same brand internationally (ii) if the FDI is proposed to be beyond 51%, then sourcing of 30% of the value of the goods purchased should be done from India, preferably from Indian micro, small, and medium enterprises.

(ii) Legal Metrology

As per the *Legal Metrology Act, 2009* (**LMA**) read with the *Legal Metrology (Packaged Commodities) Rules, 2011* (**PC Rules**), an 'e-commerce entity' is broadly defined to mean any company incorporated in India or foreign company registered in India conducting the e-commerce business. While e-commerce business is not defined under the PC Rules, the term 'e-commerce' has been defined to mean *buying and selling of goods and services including digital products over digital and electronic networks*.

[57] 15.2.3(i), Foreign Exchange Management (Non-Debt Instruments) Rules, 2019

[58] 15.2.3(h), Foreign Exchange Management (Non-Debt Instruments) Rules, 2019.

[59] 15.2.3(m), Foreign Exchange Management (Non-Debt Instruments) Rules, 2019.

While a marketplace based model of e-commerce is also required to ensure that the certain mandatory declarations are displayed on its website, the responsibility for the accuracy of the declarations are on the manufacturer/importer/seller, provided that the e-commerce marketplace complies with the due diligence requirements under the IT Act. The form/format of making such declarations is not specified under the PC Rules but based on industry practice, the same should be legible/visible on the platform.

(iii) Consumer Protection Laws:

The Ministry of Consumer Affairs, Food and Public Distribution, by way of notifications dated July 15, 2020 and July 23, 2020, notified all provisions of the Consumer Protection Act, 2019 ("**CPA**") – India's new consumer protection framework which supersedes the Consumer Protection Act, 1986. Alongside the notification of CPA 2019, the Ministry also notified the Consumer Protection (E-Commerce) Rules, 2020 ("**E-Commerce Rules**") effective July 23, 2020. The Ministry then released proposed amendments to the E-Commerce Rules in June 2021 ("**Proposed Amendment**").

The E-Commerce Rules expressly apply to all e-commerce entities operating in India, including an e-commerce entity which was not established in India but systematically offers goods or services to consumers in India. The E-Commerce Rules apply to:

- all goods and services bought or sold over digital or electronic network including digital products;
- all models of e-commerce, including marketplace and inventory models of e-commerce;
- all e-commerce retail; and
- all forms of unfair trade practices across all models of e-commerce.

a. An E-Commerce Entity

The E-Commerce Rules define "e-commerce entity" to mean "*any person who owns, operates or manages a digital or electronic facility or platform [for] e-commerce*". The term "e-commerce" is defined to mean "buying or selling of goods or services including digital products over digital or electronic network". The Proposed Amendment will broaden this definition to include "*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*".

While terms 'marketplace' and 'inventory' models have been defined, other modes of e-commerce have not been identified or defined. A "marketplace e-commerce entity" is defined as "*an e-commerce entity which provides an information technology platform on a digital or electronic network to facilitate transactions between buyers and sellers"*. On the other hand, an "inventory e-commerce entity" is defined as "*an e-commerce entity which owns the inventory of goods or services and sells such goods or services directly to the consumers and shall include single brand retailers and multi-channel single brand retailers*".

The Proposed Amendments introduce new definitions of 'cross selling,' 'fall back liability,' flash sale' and 'misselling'. E-commerce entities are sought to be prohibited from carrying out 'misselling' of goods or services. 'Misselling' has been defined as selling goods/services by deliberately misrepresenting information about the goods/services, i.e., by (1) an unwarranted positive assertion of something which is not true (2) displaying wrong information with the intent to deceive the consumer, and to the advantage of the e-commerce entity/seller, (3) causing 'however innocently' the consumer to purchase goods/services based on a mistake as to the substance of the thing being purchased.

b. Compliance Requirements

The CPA 2019 and the E-Commerce Rules impose several regulatory requirements upon 'e-commerce entities'. These are as follows:

- **Nodal Contact:** E-commerce entities who are (a) an Indian company, or (b) a foreign company as defined under Section 2(42) of the Companies Act, which then would trigger a registration requirement under the Companies Act, 2013, or (c) an office, branch or agency outside India owned or controlled by a person resident in India, as defined under Foreign Exchange Management Act, 1999 must appoint a nodal person of contact or an alternate senior designated functionary who is resident of India, to ensure compliance with the provisions of the CPA 2019 and the rules made thereunder.

- **Grievance redressal & grievance officer:** The e-commerce entity will need to name a grievance redressal officer. It will have to acknowledge and resolve the consumer complaints within specified timelines. It will also need to disclose ticket numbers to consumers to track complaints.

- **Disclosure related compliances:** The E-Commerce Rules impose certain disclosure requirements on marketplace e-commerce entities, and different disclosure requirements to sellers that operate in the marketplaces. Sellers that operate on an e-commerce marketplace must provide certain information, including the country of origin of their goods, to the marketplace e-commerce entity for display on their platforms. Further, Rule 5(2) of the E-Commerce Rules contemplates that "every marketplace e-commerce entity shall require sellers through an undertaking to ensure that descriptions, images, and other content pertaining to goods or services on their platform is accurate and corresponds directly with the appearance, nature, quality, purpose and other general features of such good or service."

c. Additional Compliance Requirements under the Proposed Amendments

The Proposed Amendments bring in a number of additional compliance requirements and prohibitions on e-commerce entities, and more specifically on marketplace e-commerce entities (MEE). The Proposed Amendments have received wide criticism and pushback from the industry, and a few of these proposed amendments are below.

- **Registration Requirement:** E-commerce entities which intend to operate in India are required to register with the DPIIT within time periods prescribed by them.

- **Additional Duties of E-Commerce Entities:** The Proposed Amendment seeks to impose several new duties on e-commerce entities, such as to ensure that sponsored listing of products and services are distinctly identified, and assist the Government with information requests in specific instances.

- **Additional Prohibitions on E-Commerce Entities:** The Proposed Amendment seeks to prohibit e-commerce entities from actions such as misleading users by manipulating search result or search indexes; permitting usage of the name or brand associated with marketplace e-commerce entities by sellers on the platform in a manner that suggests that goods or services are associated with the MEE, or organising flash sales of goods and/or services on its platform.

- **Chief Compliance Officer:** The requirement to appoint a Chief Compliance Officer (CCO) under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules) has been sought to be extended to e-commerce entities as well. The provision appears to have been reproduced almost verbatim from the IT Rules.

- **Disclosures while cross-selling:** E-Commerce entities engaged in cross-selling of goods and services, i.e., selling of goods/services which are related, adjacent or complimentary to a purchase made by a consumer at the same time, in order to maximize the entity's revenue, are required to disclose the following to their users under the Proposed Amendment:
    - Name of the entity providing data for cross-selling, and
    - Data of such entities used for cross-selling.

d. Consequences for Non-Compliance

The Proposed Amendments bring in a number of additional compliance requirements and prohibitions on e-commerce entities, and more specifically on marketplace e-commerce entities (MEE). The Proposed Amendments have received wide criticism and pushback from the industry, and a few of these proposed amendments are below.

- **Violation of the E-Commerce Rules under the CPA 2019**

  There are no direct penalties under the CPA 2019 for a) violation of the E-Commerce Rules; or b) violation of a rule or regulation framed under the CPA in general. The CPA provides for a very limited number of offences. Violation of the E-Commerce Rules should not fall under any of the listed offences.

  However, if in case of violation of the E-Commerce Rules, the Central Consumer Protection Authority (**CCPA**) could direct the violating entity[60] to undertake any compliances and should the said entities fail to do so, then such failure would amount to an offence. Before issuing such direction, the CCPA is required to follow due process specified under the CPA. Further, the said offence is compoundable, i.e., either before or after the initiation of prosecution, the first offence (within a three-year period) can be compounded by paying a prescribed fee, after which no further proceeding takes place for that offence.

- **Potential consequences of consumer complaints**

  In the event of a grievance, a consumer could file a complaint before a Consumer Commission (the dispute resolution fora, divided between the District, State and National Consumer Commissions). There is also a possibility that in case of violation of the E-Commerce Rules, a consumer may raise a complaint against an e-commerce entity for grounds such as 'misleading advertisement'.[61] The process of addressing a complaint before the Consumer Commission is detailed below:

- *Mediation*

  At the first hearing of the complaint before a Consumer Commission, the matter can be referred to mediation for settlement between the parties. If the parties cannot come to an agreement, the matter is sent back to the Consumer Commission for adjudication.

[60]Section 20, Consumer Protection Act, 2019

[61]Section 2(28), Consumer Protection Act, 2019: "misleading advertisement" in relation to any product or service, means an advertisement, which— (i) falsely describes such product or service; or (ii) gives a false guarantee to, or is likely to mislead the consumers as to the nature, substance, quantity or quality of such product or service; or (iii) conveys an express or implied representation which, if made by the manufacturer or seller or service provider thereof, would constitute an unfair trade practice; or (iv) deliberately conceals important information.

- *Potential outcomes of a matter before the Consumer Commission*

  In the event that a mediation is unsuccessful, and the Consumer Commission finds in favour of the complainant, it can pass relevant orders against the e-commerce entity.[62] Penal action is initiated only if the order of the Consumer Commission is violated. The failure to comply with an order of the Consumer Commission may lead to imprisonment for a minimum of one month and up to three years and/or fine of a minimum of INR 25,000/- and up to INR 1,00,000/-. It may be noted that an order of a Consumer Commission is appealable.

e. Judicial Challenge

Certain provisions of the E-Commerce Rules have already been challenged before the judiciary. A plea was filed by a trading proprietor challenging Rule 4(1)(a) that mandates e-commerce entities in India to be corporate entities under company law (leaving limited liability partnerships and sole proprietorships outside the scope).

In December 2020, the Delhi High Court directed the Central Government to check disclosures of 'country of origin' by e-commerce entities for products which are sold through their platforms.[63] Further, in November 2020, the Government imposed a fine of INR 25,000/- on Amazon for not displaying the country of origin on its platform.[64] The MCA had also issued notices to Flipkart and Amazon on this issue in October 2020.[65] Before the notification of the Rules, the Gujarat High Court had issued notices subsequent to the filing of a PIL on this matter.[66] This tends to show the evolving mindset of the government towards disclosing the place of origin of various goods sold in India sourced from overseas, especially given the bilateral ties with other countries.

(iv) Advertising Guidelines

The Code for Self-Regulation in Advertising (**ASCI Code**)[67] has been framed by the Advertising Standards Council of India (**ASCI**) which is a self-regulatory voluntary organisation. It specifically extends to the medium of internet. The ASCI Code is based on the principles of honest representations, non-offensiveness to the public, being against harmful products/situations, and being fair in competition. ASCI members include advertisers, the media, as well as advertising agencies.[68]

---

[62]These orders could direct e-commerce entity, including to:
a. remove the deficiencies in the services in question;
b. pay such sum as may be determined by the Commission, if it is of the opinion that loss or injury has been suffered by a large number of consumers who are not identifiable conveniently;
c. issue corrective advertisement to neutralize the effect of misleading advertisement at the cost of the opposite party responsible for issuing such misleading advertisement;
d. cease and desist from issuing any misleading advertisement;
e. provide for adequate costs to parties;
f. pay such amounts as may be determined as compensation to the consumer for loss or injury suffered due to negligence;

[63]Team, NDTV. (2020, December 10). Centre Told To Verify If All E-Commerce Firms Show Country Of Origin On Products. NDTV. https://www.ndtv.com/india-news/centre-told-to-verify-if-all-e-commerce-firms-show-country-of-origin-on-products-2336529

[64]Bureau, ET. (2020, November 25). Amazon fined for not displaying mandatory information about products. The Economic Times. https://economictimes.indiatimes.com/industry/services/retail/amazon-fined-for-not-displaying-mandatory-information-about-products/articleshow/79413590.cms?from=mdr

[65]Bhalla, T. (2020, 16 October). Consumer affairs ministry writes to Amazon, Flipkart on 'country of origin'. Livemint. https://www.livemint.com/companies/news/consumer-affairs-ministry-writes-to-amazon-flipkart-on-country-of-origin-11602868978524.html

[66]See Jalan, T. (2020, July 8). Petition in Gujarat HC seeks country of manufacture labels for e-commerce products, court issues notice. Medianama. https://www.medianama.com/2020/07/223-gujarat-hc-petition-ecommerce-country-of-manufacture/\

[67]The Code for Self-Regulation in Advertising, Advertising Standards Council of India. (1985). https://ascionline.org/index.php/ascicodes.html

[68]A list of the ASCI members can be found here: https://ascionline.org/index.php/member.html

The ASCI Code contains guidelines for advertisements of specific goods and services, such as for food and beverages, automobiles, skin lightening products, etc. It further has specific directions for celebrities in advertising. Similar to the CPA, the ASCI Code states that advertisements are not to "*distort facts nor mislead the consumer by means of implications or omissions. Advertisements shall not contain statements or visual presentation which directly or by implication or by omission or by ambiguity or by exaggeration are likely to mislead the consumer about the product advertised or the advertiser or about any other product or advertiser".*[69]

The ASCI has in place a Consumer Complaints Council (**CCC**) which considers complaints raised against advertisements, and issues recommendations to the advertiser to comply with them by either withdrawing the advertisement or modifying it. If the advertiser does not respond positively, or comply with the recommendations of the CCC within 10 days of receiving a letter from ASCI, concerned agency/media vehicles and relevant self-regulatory bodies are notified that the advertisement contravenes the ASCI Code.

Adherence to the ASCI Code has been made mandatory for advertisements on cable television, per the *Cable Television Network Rules, 1994,*[70] *framed under the Cable Television Networks (Regulation)* Act, 1995; and to broadcasters and carriers of television channels under various guidelines issued by the Ministry of Information and Broadcasting. So far as the other mediums of transmissions are concerned (i.e., digital, print, etc.), the ASCI Code is not binding under law (as they are only voluntary guidelines), but are usually adopted and followed as an industry practice.

Further, the Ministry of Consumer Affairs on September 4, 2020 released, for public comments,[71] the *draft Central Consumer Protection Authority (Prevention of Misleading Advertisements and Necessary Due Diligence for Endorsement of Advertisements) Guidelines, 2020* on prevention of misleading advertisements. In addition to prescribing conditions for an advertisement to be 'valid', the guidelines also impose various duties on endorsers, experts, service providers and advertising agencies to conduct their diligence and ensure that the claims they make in advertisements are truthful.

The said guidelines have not been notified as of date, though it is interesting to see the Indian Government take a firmer stance against misleading advertisements and unfair trade practices, and place responsibilities and corresponding liabilities on experts and endorsers, often celebrities with mass fan followings, that may be involved.[72]

(v) Social Media Influencer Guidelines

In February 2021, ASCI issued draft guidelines on *Advertising by Social Media Influencers*[73] ("**Influencer Guidelines**"). ASCI notes that with the lines between content and advertisements becoming blurry, it is critical that consumers must be able to distinguish when something is being promoted with an *intention to influence their opinion or behaviour for an immediate or eventual commercial gain*. When consumers view

[69]Paragraph 1.4, ASCI Code

[70]Rule 7(9) of the Cable Television Network Rules 1994 states: "*No advertisement which violates the Code for self- regulation in advertising, as adopted by the Advertising Standard Council of India (ASCI), Mumbai, for public exhibition in India, from time to time, shall be carried in the cable service.*"

[71]The Central Consumer Protection Authority (Prevention of Misleading Advertisements and Necessary Due Diligence for Endorsement of Advertisements) Guidelines, 2020. https://consumeraffairs.nic.in/sites/default/files/file-uploads/latestnews/Draft%20guidelines%20for%20stakeholders%20consultation.pdf

[72]Tewari, S. (2021, 28 July). ASCI to send notice to Virat Kohli over Lovely Professional University Post. Livemint. https://www.livemint.com/industry/advertising/asci-to-send-notice-to-virat-kohli-over-lovely-professional-university-post-11627462302082.html

[73]The Influencer Guidelines define an Influencer as someone *who has access to an audience and the power to affect their audience's purchasing decisions or opinions about a product, service, brand or experience, because of the influencer's authority, knowledge, position, or relationship with their audience, An influencer can intervene in an editorial context or in collaboration with a brand to publish content*.

promotional messages without realising its commercial intent, the messages become inherently misleading.

In summary, the draft Influencer Guidelines suggest that influencers must add detailed disclosures to their posts, do their due diligence about any technical or performance claims in the products or services they promote, and that the contractual agreement between advertiser and influencer carries clauses pertaining to disclosure, use of filters as well as due diligence.

ASCI will issue a notice to both brand owner and influencer for violation of the guidelines in the case of a consumer complaint or *suo motu* cognisance of a potentially objectionable advertisement.

(vi) Government Engagement of Social Media for Ads

The Ministry of Information and Broadcasting ("**MIB**") in May 2020, published Policy Guidelines for Empanelment of Social Media Platforms with the Bureau of Outreach and Communication.[74] The guidelines apply to Government's engagement of social media platforms so that an assured reach could be attained (on a payment basis) to increase visibility of socially relevant messages. The guidelines prescribe eligibility criteria for social media platforms including continuous operation under the same domain name for at least six months and minimum of 25 million unique users from within India per month. Social media platforms would need to go through a bidding process for empanelment and be subject to the broad terms of agreement and pricing mechanics as set out by the MIB in the said policy guidelines.

(vii) Rules for Intermediaries and Publishers of Online Curated Content

The Ministry of Electronics and Information Technology ("**MeitY**") *notified the Information Technology [Intermediary Guidelines and Digital Media Ethics Code] Rules, 2021* ("**2021 Rules**") on February 25, 2021. The 2021 Rules supersede the *Information Technology (Intermediaries Guidelines)* Rules, 2011 ("2011 Rules") and expands the scope of due diligence and compliance requirements on intermediaries and introduces obligations on publishers in relation to online content (including news/current affairs and curated content).

Overall, the drafting of the 2021 Rules is not meticulous, certain definitions lack clear articulation, the nature of content that it seeks to regulate, and applicable compliance requirements are not completely clear. There is also a possible scope of argument that some provisions of the 2021 Rules are *ultra vires* IT Act (under which it is issued) such as the ability to block/modify content on publishers' websites by the Ministry of Information and Broadcasting ("**MIB**").

The 2021 Rules seek to regulate the following categories of businesses:

1. 'Intermediaries, such as telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces, etc. Intermediaries also include:
    a. Social Media Intermediaries (SMI), and
    b. subset of SMIs termed Significant Social Media Intermediaries (SSMI); and

[74]Policy Guidelines for Empanelment of Social Media Platforms with Bureau of Outreach and Communication, Ministry of Information and Broadcasting. (2020, May). https://mib.gov.in/sites/default/files/PolicyGuidelinesforSocialMediaPlatforms2020.pdf

2. Publishers of News and Current Affairs Content ("**NCAC**")[75] [76] (which include news aggregators); and
3. Publishers of Online Curated Content ("**OCC**")[77] [78] (which includes individual creators).

a. Concept of an 'Intermediary'

The IT Act defines an intermediary, with respect to any particular electronic records, as "***any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record*** *and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes*".

b. 'Social Media Intermediaries' and 'Significant Social Media Intermediaries'

The IT Act defines an intermediary, with respect to any particular electronic records, as "***any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record*** *and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes*".

- Social Media Intermediaries (SMIs)

  SMIs are defined as intermediaries which primarily or solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using their services.

- Significant Social Media Intermediaries (SSMIs)

  An SSMI is defined to mean an SMI having a number of registered users in India above the threshold prescribed by the Central Government. MeitY, vide a notification issued on February 26, 2021, has provided that this threshold is **50 lakh (5 million) registered users**. It is unclear as to how this threshold would be determined, i.e., whether a 'registered' user includes those who don't open an account on the intermediary's platform but still use the platform. The 2021 Rules do not provide for a definition of the term 'registered user'. There may also be some practical challenges for SMIs above and below the prescribed registered-user number, as their status would fluctuate periodically between that of an SMI and an SSMI. This would lead to difficulty in implementing a compliance system.

---

[75]Rule 2(1)(m) defines news and current affairs content as including "newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks, and any digital media shall be news and current affairs content where the context, substance, purpose, import and meaning of such information is in the nature of news and current affairs content."

[76]Rule 2(1)(t) defines publisher of news and current affairs content as "an online paper, news portal, news aggregator, news agency and such other entity called by whatever name, which is functionally similar to publishers of news and current affairs content but shall not include newspapers, replica e-papers of the newspaper and any individual or user who is not transmitting content in the course of systematic business, professional or commercial activity."

[77]Rule 2(1)(q) defines online curated content as "any curated catalogue of audio-visual content, other than news and current affairs content, which is owned by, licensed to or contracted to be transmitted by a publisher of online curated content, and made available on demand, including but not limited through subscription, over the internet or computer networks, and includes films, audio visual programmes, documentaries, television programmes, serials, podcasts and other such content."

[78]Rule 2(1)(u) defines publisher of online curated content as "a publisher who, performing a significant role in determining the online curated content being made available, makes available to users a computer resource that enables such users to access online curated content over the internet or computer networks, and such other entity called by whatever name, which is functionally similar to publishers of online curated content but does not include any individual or user who is not transmitting online curated content in the course of systematic business, professional or commercial activity."

- Safe Harbour: Under Section 79 of the IT Act[79], intermediaries are accorded 'safe harbour' from liability for content published by third parties and hosted on their platform, subject to the intermediary observing due diligence while discharging their duties.[80]

  The 2021 Rules clarify that where an intermediary fails to observe the rules, they cannot avail safe harbour under Section 79, and may be held liable for third party content on their platform under the content laws (i.e., for such as the Indian Penal Code, 1860, which makes publication of certain categories of information criminal offences).

c. Challenges to the 2021 Rules

There have been a number of challenges filed against the 2021 Rules, as listed below:

Delhi HC: *The Foundation for Independent Journalism*, owner of the digital news portal The Wire, filed a writ petition against the IT Rules on March 6, 2021 in order to declare them *ultra vires* the IT Act.[82] The grounds for challenge were that the 2021 Rules go beyond the scope of the IT Act by seeking to regulate 'digital news portals' via the classification of '*publishers of news and current affairs content*' and for seeking said digital news under the Code of Ethics and Procedure and Safeguards in Relation to Digital Media, i.e., Part III of the Rules.

10 days after this petition, *Quint Digital Media Ltd*, also filed a petition, claiming that the IT rules are in violation of Articles 14, 19(1)(a), 19(1)(g) and 21.[83] The third case was filed by Pravda Media Foundation wherein

---

[75]Section 79: Exemption from liability of intermediary in certain cases. –
1. Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.
2. The provisions of sub-section (1) shall apply if-
   (a) The function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or
   (b) the intermediary does not-
      (i) initiate the transmission,
      (ii) select the receiver of the transmission, and,
      (iii) select or modify the information contained in the transmission;
   (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.
3. The provisions of sub-section (1) shall not apply if-
   (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or othorise in the commission of the unlawful act;
   (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation. -For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.]

[80]Section 79(2)(c), Information Technology Act, 2000: the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

[81]Rule 7, Information Technology [Intermediary Guidelines and Digital Media Ethics Code] Rules, 2021.

[82]*Foundation for Independent Journalism & Ors. v Union of India & Anr*, Writ Petition (C)No. 3125 of 2021

[83]*Quint Digital Media Limited & Anr v Union of India & Anr*, Writ Petition (C) No. 3659 of 2021

the Court on June 28, 2021 refused to grant them interim relief.[84] On July 7, 2021, news portals The Wire, The Quint and AltNews were also refused interim relief. At the same time, on July 8, 2021, a new case was filed by the Press Trust of India for interim protection which the bench refused to grant.[85]

The Delhi HC on June 28, 2021 refused to stay the Centre's notice to digital news portals to comply with the IT Rules.[85]

Bombay HC: Challenges were filed here by journalist Nikhil Mangesh Wagle, on July 1, 2021 and a digital news portal, *AGIJ Promotion of Nineteenonea Media Pvt. Ltd.* on July 9, 2021.[86] In a significant development, the Bombay High Court passed an interim stay on the operation of Rule 9(1) and 9(3) on August 14, 2021. The Court stayed their operation on two grounds:

- They imposed an obligation on publishers to abide by the Code of Ethics provided in a completely different statutory regime, i.e., print journalism and cable TV. The court stated that S. 87 of the IT Act did not empower the government to impose these compliances on publishers. The Code of Ethics placed the Norms of Journalistic Conduct framed by the Press Council of India ("**Norms**") to a status of mandatory compliance despite the sanction of the Norms being moral and not statutory.

- Secondly, Rule 9 *prima facie* infringed the fundamental right to freedom of speech granted by Article 19(1)(a), by requiring publishers to comply with the Norms.

Madras High Court: TM Krishna and Digital News Publishers Association, filed petitions before the Madras High Court which comprises of over 13 media outlets.[87] They identified themselves as '*legacy media houses*', and differentiated themselves from the '*digital media*' mentioned in the Rules, since they only run online portals whereas the petitioners ran newspapers and news channels and would not come under the new rules. The Court passed an order on September 16, 2021 where it held that the Bombay High Court order, mentioned above, ought to have a pan-India effect, and ordered that Rules 9(1) and 9(3) ought to be stayed. The Madras High Court also noted in its interim order that any action taken citing Rules 3 and 7 of the IT Rules 2021 would be subject to the outcome of the challenge to the writ petition.

Kerala High Court: There were two major challenges filed here regarding digital news portals and in both cases, interim protection was granted. The first case was filed by LiveLaw News Media Pvt Ltd, on 10 March, 2021 wherein the bench passed an order restraining any coercive action being taken against the petitioners.[88] In the second case, the court passed an order based on the prior case and accordingly interim protection was granted to the News Broadcasters Association.[89]

Transfer to Supreme Court: The Centre has now filed a transfer petition in the Supreme Court to avoid multiplicity of proceedings and transfer four of the several petitions filed in various High Courts.[90] The petition does not seek transfer of the cases involving social media intermediaries. Notably, the Supreme Court did not stay the order of the Kerala High Court, restraining the government from taking any coercive action against LiveLaw under Part III of the Rules. They also did not order a stay on the proceedings pending before various High Courts despite the centre's request.

---

[84] *Pravda Media Foundation v Union of India & Anr*, Writ Petition (C) No. 5973 of 2021; Sanjay Kumar Singh v UOI, Writ Petition (C) No. 3483 of 2021.

[85] *Press Trust of India v Union of India*, Writ Petition (C) No. 6188 of 2021.

[86] *AGIJ Promotion of Nineteenonea Media Pvt. Ltd. & Ors. v Union of India & Anr,* Writ Petition (L.) No. 14172 of 2021; Nikhil Mangesh Wagle v UOI, PIL (L.) No. 14204 of 2021

[87] *Digital News Publishers Association & Anr v Union of India & Anr*, Writ Petition No. 13055 of 2021; T.M Krishna v UOI

[88] *Live Law Media Pvt Ltd v Union of India*, Writ Petition (C) No. 6272 of 2021.

[89] *News Broadcasters Association v. Ministry of Information and Broadcasting*, Writ Petition (C) No. 14239 of 2021

[90] *UOI v. Foundation for Independent Journalism & Ors.*, Transfer Petition (Civil) No. 997-1000 of 2021.

(viii) Payment laws

The Reserve Bank of India (RBI) regulates payment systems through the Payment and Settlement Systems Act, 2007 ("**PSS Act**"). Pursuant to the PSS Act, the RBI has issued Guidelines on Payment Aggregators and Payment Gateways, dated March 17, 2020 ("**PA/PG Guidelines**"). The RBI further issued clarifications on the PA/PG Guidelines, dated September 17, 2020 ("**PA/PG Clarifications**").

- Requirement of registration for PAs

  The PA/PG Guidelines require payment aggregators ("**PAs**") to be licensed by the RBI. They must also be incorporated in India. The PAs are defined as entities that "*receive payments from customers, pool and transfer them on to the merchants after a time period*." Neither the PSS Act nor the PA/PG Guidelines have extraterritorial applicability, and the PSS Act only extends to India.

- Restrictions on storing card data

  The PA/PG Guidelines, read with the PA/ PG Clarifications, prohibit merchants and PAs from storing '*customer card and related data*'. PAs are required to ensure that neither they, nor merchants, store customer card credentials (except, limited information for transaction tracking). They are also required to ensure that merchants do not store any 'payments data' except 'limited data' for purposes of transaction tracking. The term "merchant" has not been defined in the PA/PG Guidelines. However, in the PA/PG Clarifications, the RBI specified that 'e-commerce entities' availing the services of a PA are 'merchants' under the PA/PG Guidelines.

  The term 'payment data' is also not defined in the PA/PG Guidelines. However, in the context of data localisation (DL) in India, the RBI has clarified that "payment credentials" (including card information) are a subset of 'payment data'. Therefore, drawing reference from the clarification issued by the RBI under the DL FAQs *(defined below)* in relation to scope of 'payment data', customer card credentials may be viewed to be covered within the ambit of 'payment data' as used in the PA/ PG Guidelines and the PA/ PG Clarifications.

- Exemption for "delivery v. payment" and "postpaid" transactions

  The PA/PG Clarifications state that the PA/PG Guidelines "shall not apply to '*Delivery v. Payment' transactions but addresses transactions where payment is made in advance while the goods are delivered in a deferred manner*". (Clause 1(d)). "'Delivery v. Payment' transactions" ("**DvP**") are transactions where the customer receives goods/services immediately/simultaneously upon making the payment. Postpaid transactions are transactions where goods/services are delivered before the payment is made by the customer.

- E-Mandate Circulars

  The RBI requires banks to obtain from their customers an additional factor authentication ("**AFA**") (typically a 'one time pin') for all online transactions which are above specified monetary thresholds of INR 5,000/- (including credit/ debit card transactions) in Indian Rupees. The RBI issued two circulars in August 2019 and December 2020 ("**E-Mandate Circulars**") that alter this scheme for certain '*recurring payments*' The circulars are not applicable to 'once-only' transactions, which still require an AFA for each payment transaction. The RBI has specified that transactions not compliant with the circulars shall not be facilitated beyond March 31, 2021. This regime went live from October 1, 2021, but as per our understanding not all banks were prepared with the required technology integrations to effect recurring payments under the new regime.

The E-Mandate Circulars prescribe the following rules for recurring payments:

- The maximum limit for recurring payments is INR 5,000/- per transaction.

- For recurring transactions under the maximum limit, a cardholder has to authorise a one-time mandate with the issuing bank (i.e. an instruction given to the issuing bank to release payments when charged by the merchant). No further AFA is required for the recurring payments unless the cardholder seeks to modify the authorised mandate or the transaction exceeds the INR 5,000/- limit. However, the card issuing bank of the customer is required to send a 24-hour advance notice of each recurring charge allowing the customer to opt-out of making that payment.

The E-Mandate Circulars have been addressed to the RBI-regulated banks, card payment networks, and prepaid instrument issuers who will have to ensure compliance. The E-Mandate Circulars (issued in terms of the PSS Act) do not have any provisions for extra-territorial applicability.

- DL Circular and DL FAQ

  The RBI issued a circular on 'Storage of Payment System Data' dated April 6, 2018 ("**DL Circular**"), read with the RBI Frequently Asked Questions on Storage of Payment System Data issued in July 2019 ("**DL FAQ**"). The DL Circular requires RBI-regulated payment system providers to "ensure that the entire data relating to payment systems operated by them are stored in a system only in India." This 'data' is defined to include 'the full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction.'

  The DL FAQ states that 'the directions are also applicable in respect of the transactions through system participants, service providers, intermediaries, payment gateways, third party vendors and other entities (by whatever name referred to) in the payments ecosystem, ***who are retained or engaged by the authorised / approved entities for providing payment services***.'

  In the event of a cross border transaction, the DL Circular permits data in relation to the ***foreign leg*** of the transaction to be stored overseas. If there is a domestic component, 'a copy of the domestic component may also be stored abroad, if required.'

- CNP Circular

  The RBI issued a circular on 'Security Issues and Risk mitigation measures related to Card Not Present (CNP) transactions' dated August 22, 2014 ("**CNP Circular**"). The CNP Circular addresses the issue of online card transactions where the 'underlying transactions are essentially taking place between ***two residents in India*** (cards issued in India being used for purchase of goods and services offered by a merchant/service provider in India)'. It provides:

- where cards issued by banks in India are used for making card-not-present payments towards purchase of goods and services provided within the country, the acquisition of such transactions has to be through a bank in India and it should necessarily settle only in Indian currency; and

- an AFA is required for such payments.

- OPGSP Circular

  The RBI issued a circular on 'Processing and settlement of import and export related payments facilitated by Online Payment Gateway Service Providers' dated September 24, 2015 ("**OPGSP Circular**"). The OPGSP Circular allows banks to partner with third parties known as Online Payment Gateway Service Providers ("**OPGSPs**") to facilitate cross-border payments. The Circular allows such payments to be collected from an Indian payer in rupees, while the payout is enabled by the bank and OPGSP to the foreign recipient in foreign currency. Vice versa, the Circular allows payments from a foreign payer to be made in foreign currency to an OPGSP and its partner bank, who will settle the payment to the Indian payee in Indian rupees.

  The OPGSP Circular has the following key restrictions:

  - Outward remittances from India can be made for imports of goods and software only, and up to a maximum limit of USD 2,000/-.

  - Inward remittances to India can be made for exports of goods and services, and up to a maximum limit of USD 10,000/-.

(ix) E-Contracts

E-commerce entities for the most part, conduct their sales, and hence enter into e-contracts. The IT Act provides validity to contracts formed through electronic means.[91] Hence, concluding contracts in electronic form or via electronic records[92] is valid as per the IT Act, if the contract is otherwise enforceable under contract law. Such contracts should be legally valid and are akin to physical contracts.

(x) IP Protection

One of the foremost considerations that any company intending to commence e-commerce activities should bear in mind is the protection of its intellectual assets. The internet is boundless with minimum regulation and therefore the protection of intellectual property rights ('IP' or 'IPR') is a challenge and a growing concern amongst most e-businesses. Some of the significant issues that arise with respect to protecting IPRs in e-commerce are discussed hereunder.

Is there a protectable Intellectual Property?

Traditionally inventions, literary works, artistic works, designs and trademarks formed the subject matter of earlier intellectual property law. However, with the advent of new technologies, new forms of IPRs are evolving and the challenge for any business would be in identifying the various options for protection of its intellectual assets. Some of the main forms of intellectual property protection that an e-commerce business would be concerned about are as follows:

- Copyrights for protection of the content, design of the websites, the software underlying the platform and the content transmitted over such platforms.

---

[91]*Section 10A - Validity of contracts formed through electronic means – where in a contract formation, the communication of proposals,* ***the acceptance of proposals, the revocation of proposals*** *and acceptance as the case may be,* ***are expressed in electronic form or by means of an electronic record,*** *such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.*

[92]*Section 2(t) of the IT Act defines 'electronic record' as:* ***"…data, record or data generated****, image or sound stored,* ***received or sent in an electronic form*** *or computer generated micro fiche."*

- Trademarks to protect the words, taglines or logos with which any person would identify with the e-commerce platform/ business. In addition to protecting their own trademarks, an e-commerce business that sells or markets other brands on its portal would have to ensure that such business' trademarks are protected as well.
- Patents to protect (where allowed by law) the functionality of the software and the methods underlying such e-commerce. In India, there is no patent protection for computer programs per se, and hence there is a need to look at alternate methods to protect software.

Common Issues with respect to IP in E-Commerce

When any e-commerce platform is created, the enterprise should use either proprietary or validly licensed technology.

a. Designing a Platform / Content Creation Through a Third Party

One of the most common scenarios where the question of ownership of IP arises is in the context of the website/ platform on which the business is carried out. Often e-commerce companies outsource the job of designing such websites/platforms or creation of content to third party contractors. The issue here would be, who would own the IP in the design and functionality (software underlying the website) of the website and in the content.

b. Hyperlinking, Framing and Meta Tagging

An important consideration for e-commerce companies is their ability to market their business and their ability to constantly adapt and use technology to serve that purpose. In pursuit of achieving such marketing goals, e-commerce businesses sometimes have to deal with hyperlinking, deep linking,[93] framing[94] and meta tagging[95] issues, and it is important to understand the legal implications of the same. Courts in many countries are grappling with issues concerning all of the above-mentioned activities. Courts in certain jurisdictions have held that hyperlinking; especially deep hyperlinking may constitute copyright infringement, whereas meta tagging may constitute trademark infringement.[96]

c. Fair Dealing

In the context of an e-commerce business there is less likelihood of fair use defence available since commercial benefit is the underlying purpose of an e-commerce business.

d. Domain Names

A company that commences e-commerce activities would at first have to get its domain name registered. Domain names normally fall within the purview of trademark law. The Indian courts have been proactive in granting orders against the use of infringing domain names.[97] The take away from all these cases is that

[93]Hyperlink is a reference to a webpage or document on the Internet and deep hyperlink links to a specific interior page or paragraph inside a website surpassing the homepage.

[94]Framing is the juxtaposition of two separate web pages within the same page.

[95]Metatags are HTML codes that are intended to describe the contents of a web page but do not appear on the web page.

[96]Elgison, M.J., & Jordan, J.M. (1998). *Trademark Cases Arise from Meta-Tags, Frames: Disputes Involve Search-Engine Indexes, Web Sites within Web Sites, as well as Hyperlinking*. National Law Journal. http://cyber.law.harvard.edu/property00/metatags/mixed1.html

[97]Some of the cases in which injunctions against the use of conflicting domain names have been granted are: *Yahoo Inc. v Aakash Arora & Anr*, AIR 2000 Bom 27; *Rediff Communication v Cyberbooth & Anr*, 1999 PTC (19) 201 and *Satyam Infoway Ltd. v Sifynet Solutions Pvt. Ltd.*, AIR 2004 SC 3540.

domain name serves the same function as a trade mark, and is not a mere address or like finding number on the internet, and therefore, it is entitled to equal protection as a trademark and that even an action for passing off can be filed for domain names.

e. Enforcing IP - Liability for Infringement of IP

There are a host of factors that a court would consider in deciding whether or not there is an infringement of copyright or trademark or as the case may be. Some of the most common forms of liability for infringement in India would be:

- Injunction (temporary or permanent) against the infringer stipulating that the infringing activity shall not be continued.
- Damages to the extent of lost profit or damages to remedy unjust enrichment of the infringing party.
- Order for accounts of profits.
- Order for seizure and destruction of infringing articles.

In addition to the civil remedies, some of the IP laws contain stringent criminal provisions relating to offences and penalties such as imprisonment of up to three years for applying for a false trademark[98], knowingly infringing a copyright[99] and for applying for a false geographical indication.[100]

(xi) Blocking Orders

The Indian Government over the last year has blocked 200+ mobile applications offered by Chinese developers from access and download by users in India. MeitY invoked its power under Section 69A of the IT Act supplemented by the *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules)* to issue these orders. The blocking of the apps extends to mobile and non-mobile internet-enabled devices. Some of the blocked apps include AliExpress, AliPay, Helo, TikTok, SHAREit, UC Browser, Club Factory, WeChat, and Shein. MeitY, via press releases dated 29t June,[101] 2 September,[102] and 24 November, 2021,[103] informed the public of the blocking of the apps.

The blocking stems from rising tensions between the Indian and Chinese Governments. MeitY in its press releases mention that this was done based on information it received that the said apps were engaged in activities 'prejudicial to the sovereignty and integrity of India, defence of India, security of the state and public order'. The app block also appears to be a cue to promote home-grown technological innovation and solutions. The Indian Government has since been increasingly promoting locally developed apps.

---

[98]Section 103, The Trademark Act, 1999.

[99]Section 63, The Copyright Act, 1957.

[100]Section 39, The Geographical Indication of Goods Act, 1999.

[101]Ministry of Electronics and Information Technology. (2020, June 29). *Govt bans 59 apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order* [Press Release]. https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206

[102]Ministry of Electronics and Information Technology. (2020, September 2). *Government blocks 118 Mobile Apps which are* prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order [Press Release]. https://pib.gov.in/PressReleasePage.aspx?PRID=1650669

[103]Ministry of Electronics and Information Technology. (2020, November 24). *Government of India blocks 43 mobile apps from accessing by users in India* [Press Release]. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1675335

(xii) PILs re. to Online Content and OTT Platforms

There have been multiple PILs filed against OTT content streaming platforms in respect to the broad theme on regulation of online content. The issue is currently pending[104] before the Supreme Court of India ("**Supreme Court**").

A petition[105] with a similar issue was filed before the High Court of Bombay (Nagpur Bench). The High Court has listed the matter as a 'sine die' matter since the Supreme Court is already seized of this issue. Further, petitions seeking the regulation of online content are also pending before the High Courts in Madhya Pradesh, Madras and Punjab & Haryana.[106]

Given that the issue is pending before various courts, the Union of India has filed a transfer petition seeking a transfer of all the pending matters to the Supreme Court. If the petition is allowed, the Supreme Court will adjudicate upon this issue.

(xiii) E-Commerce Policy

A draft of the new e-commerce policy was reportedly leaked in July 2020, and proposed to set up an e-commerce regulator with wide-ranging powers over e-commerce entities and platforms. The draft stated that while there was no universally accepted definition of e-commerce, '*given the evolving nature of transactions, e-commerce will include buying, selling, marketing, distribution or providing access to (i) goods, including digital products, or (ii) services; through any electronic network for a price*.' The draft also contained wide-ranging proposals on sharing source codes, algorithms and other data with the Government, use of non-personal data of consumers, anti-piracy, cross border data flows, etc.

As per more recent media reports,[107] the Indian Government is in the 'final stages' of drafting India's e-commerce policy, which is expected to be a "robust framework".[108] It would be interesting to see whether many of the data related provisions such as on ownership, the Government access and data sharing have been diluted, in light of the industry feedback and in the backdrop of the impending personal data protection law and non-personal data protection framework currently under the Government's consideration.

---

[104] *Justice for Rights Foundation v Union of India &Ors.* SLP(C) No. 010937/2019; *Shashank Shekhar Jha v Union of India & Anr.* Writ Petition (C) No. 1080 of 2020.

[105] *Divya Ganeshprasad Gontia v Union of India & Ors.*, PIL No. 127 of 2018.

[106] 1) *Maatr Foundation v Union of India*, Writ Petition No. 18801 of 2019. (Madhya Pradesh at Indore); (2) Writ Petition No. 10180 of 2020. (Madras); (3) *Gurdeepinder Singh Dhillon v Union of India and Others*, Civil Writ Petition No. 8089 of 2020. (Punjab)

[107] Online, FE. (2020, October 28). Govt: E-commerce policy in 'final stages' of drafting; retail trade policy to benefit 65m small traders. *Financial Express*. https://www.financialexpress.com/industry/sme/govt-e-commerce-policy-in-final-stages-of-drafting-retail-trade-policy-to-benefit-65m-small-traders/2115990/

[108] Bureau, ET. (2021, October 3). Proposed e-commerce policy to be robust, balanced, says Piyush Goyal. *The Economic Times*. https://economictimes.indiatimes.com/news/economy/policy/proposed-e-commerce-policy-to-be-robust-balanced-says-piyush-goyal/articleshow/86729490.cms

B. Data Protection

(i) Information Technology Act, 2000

Data protection in India is currently governed by the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 issued thereunder ("**Data Protection Rules**"). Apart from the IT Act and Data Protection Rules, there are certain sector-wise data protection obligations and requirements, for instance in the telecommunications, insurance and banking and financial services sectors. An example is the DL circular mentioned in Chapter III.

It is pertinent to note that the compliance requirements under the Data Protection Rules have been stated by the Government of India to be applicable to Indian entities only. However, the IT Act has extraterritorial jurisdiction, if certain nexus requirements to India are met, and in certain cases non-Indian entities could be penalised for their negligence in handling certain sensitive personal data, as mentioned below.

a. Data Protection Rules

The Data Protection Rules have provisions dealing with the protection of two classes of information set out below:

- Personal Information ('PI'): which is defined as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person. As such, PI could mean any information that identifies a person such as his/her name, address, phone number etc.

- Sensitive personal data or information ('SPDI') which consists of the following items of personal information which can identify a natural person: password; financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; and biometric information.

There are no specific compliances set out in the IT Act or the Data Protection Rules applicable to an entity dealing with PI which does not amount to SPDI. However, the Data Protection Rules set out compliances for an entity located in India that collects, stores, processes, discloses or transfers SPDI, such as to take the individual's consent for the purpose of usage, give notice of collection, adopt an agreed-to privacy policy, appoint a grievance officer, undertake and adopt reasonable security procedures and practices for the information, to name a few.

b. Penalties

Section 43A: If the data collector or processor is negligent in implementing and maintaining the reasonable security practices and procedures as described under the Data Protection Rules in relation to any SPDI, which may cause wrongful loss to any person, then the collector/processor may be liable to pay damages by way of compensation to the affected person under Section 43A of the IT Act. The amount of such compensation will be determined by the enforcement agency. Even if there is a breach of the security requirements as prescribed under the Data Protection Rules without wrongful loss having been caused to a person, the entity may still be penalised under the IT Act to a relatively nominal extent.

Section 72A of the Act penalises disclosure of personal information if the following prerequisites are fulfilled:

- The person or intermediary gained access to material containing personal information while providing services under the terms of a lawful contract;
- With the intent of causing or knowing that they are likely to cause wrongful loss or gain;
- Discloses information without the consent of the person concerned or in breach of contract.

The penalty for the same is imprisonment up to three years or with a fine of up to five lakh rupees or both.

The IT Act also penalises several cyber crimes:

- Charging the services availed by one person to the account of another person[109];
- Tampering with computer source documents or knowingly or intentionally concealing, destroying or altering any computer source code, etc. when it's meant to be maintained by the law. The person having tampered with such software need not be entrusted with the same to be held liable;
- Violation of user privacy by intentionally capturing, publishing or transmitting the image of a private area of a person without their consent[110];
- Cyber terrorism i.e., intent to threaten the unity integrity or sovereignty of India or to strike terror[111]; Dishonestly receiving stolen computer resource or communication device[112],
- Punishment for identity theft[113],
- Publishing or transmitting obscene material[114], material containing sexually explicit acts etc.; and material depicting children in sexually explicit acts[115],
- Breach of confidentiality and privacy[116];
- Publishing a false Digital Signature Certificate for fraudulent or other unlawful purposes.[117]

By virtue of their business models, e-commerce entities collect vast amounts of PI, which may include SPDI. In the absence of a dedicated data protection law which deals with handling and processing of all PI, not limited to SPDI, it is important to institute industry practices so as to ensure protection of personal data. As

[109]Section 43(h), Information Technology Act, 2000

[110]Section 66E, Information Technology (Amendment) Act, 2008

[111]Section 66F, Information Technology (Amendment) Act, 2008.

[112]Section 66B, Information Technology Act, 2000.

[113]Section 66C, Information Technology Act, 2000

[114]*Section 67, Information Technology Act, 2000.*

[115]Section 67B, Information Technology Act, 2000.

[116]Section 72, Information Technology Act, 2000

[117]Sections 73 and 74, Information Technology Act, 2000

covered below, India is in the process of instituting a stringent data protection law, which will entail a much higher compliance burden for all entities in the e-commerce ecosystem, and those that generally collect and process personal data.

(ii) Data Breach Reporting Requirements

Current data breach reporting requirements in India hinge on whether a 'cyber security incident' took place, and not on whether any personal data was involved in the breach. We explain these reporting requirements below. However, the PDP Bill, if enacted in its current form, will bring in a parallel data breach reporting requirement for any breaches of personal data, as well as potentially, of non-personal data.

The Computer Emergency Response Team (CERT-In) is India's nodal agency formed under Section 70B of the IT Act and is responsible for being the first responders for any cyber security incident. Its vision is to focus on taking proactive measures to secure India's cyber space. The functions and responsibilities of CERT-In, are laid down under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT Rules).

Rule 12 of the CERT Rules provide that service providers, intermediaries, data centres, and body corporates should report 'cyber security incidents' to CERT-In within a reasonable time of occurrence or noticing the incident to have scope for timely action. Hence, should a breach/incident constitute a 'cyber security incident',[119]it would need to be reported to CERT-In.[120] Details regarding methods and formats for cyber security reporting and vulnerability reporting are published on the website of CERT-In.[121]

(iii) Data Protection Bill, 2021

Following the judgement by the Supreme Court in the case of *Justice KS Puttaswamy v. Union of India*[122] and the report submitted by Justice B N Srikrishna Committee on Data Protection,[123] the Personal Data Protection Bill, 2019 (**"PDP BIII"**) was introduced to regulate the "flow and usage of personal data".[124] The PDP Bill was subsequently referred to the Joint Parliamentary Committee ("**JPC**"). Recently, the JPC has submitted its report to both the parliamentary houses with their recommendation.

---

[118]Indian Computer Emergency Response Team, https://www.cert-in.org.in

[119]A 'cyber security incident' is defined under the CERT Rules as "any real or suspected adverse event in relation to cyber security[1] that violates an explicitly or implicitly security policy resulting in unauthorized access, denial of service or disruption, unauthorized use of a computer resource for processing or storage of information or changes to data, information without authorization. 'Cyber security' is further defined under the IT Act as "protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction."

[120]The types of cyber security incidents that mandatorily need to be reported to CERT-In are: Targeted scanning/probing of critical networks/systems 2. Compromise of critical systems/information 3. Unauthorised access of IT systems/data 4. Defacement of website or intrusion into a website and unauthorised changes 5. Malicious code attacks 6. Attacks on servers 7. Identity theft 8. Denial of Service and Distributed Denial of Service attacks 9. Attacks on Critical Infrastructure, SCADA Systems and Wireless Networks 10. Attacks on Applications such as E-Governance, E-commerce

[121]Cert-in, *supra* note 127.

[122](2017) 10 SCC 1.

[123]Committee of experts under the chairmanship of Justice B.N Srikrishna. (2018). *Free and Fair Digital Economy: Protecting Privacy, Empowering Indians.* Ministry of Electronics & Information Technology. http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

[124]The Personal Data Protection Bill, 2019. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Certain key changes that the PDP Bill would introduce are: compliance requirements for the collection and processing of all personal data (and not just SPDI as under the existing regime), data transfer restrictions and compliances, and limited data localisation requirements. Importantly, the PDP Bill is designed to have extra-territorial application and is linked to the processing of personal data by entities not present within the territory of India; if such processing is '*(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to Data Principals within the territory of India; or (b) in connection with any activity which involves profiling of Data Principals within the territory of India*'. Further, the PDP Bill will reportedly broaden its scope to govern not only personal data, but also non-personal data.

The JPC has proposed an all encompassing legislation which will govern personal as well as non-personal data. The report has made its recommendation based on the economic potential that data offers and identifies data as an 'asset of national importance' and focuses on the need to unify data sets. It is on these parameters that the Committee has included non-personal data in the legislation as well. In continuation from the previous version of the Bill, the JPC report retained strict data localisation requirements with an objective to protect national security interests, privacy and generating employment. India's Data Protection Bill requires the mirroring of copies of the sensitive data to be stored in India and restricting the transfer and processing of critical personal data abroad. In fact, non personal data has also been included in the proposed legislation and towards that Clause 92(2) which mandates sharing of non-personal data including anonymised datasets with the government.

(iv) Proposed Framework on Non-Personal Data

Separately, a committee constituted by the Ministry of Electronics and Information Technology to explore the governance of non-personal data ('NPD'), released a second and revised report[124] with their recommendations and the establishment of a separate, and independent, NPD framework. The Committee invited stakeholders to submit their suggestions and feedback on the report in January 2021.

Importantly, the Committee clarified that the scope of the PDP Bill should be distinct from the NPD framework, and further recommended that the PDP Bill be amended to remove all provisions that deal with NPD. This suggestion is currently in conflict with the report of JPC which seeks to bring PDP and NPD under an umbrella law and have recommended to expand the scope of PDP to cover NPD as well.

Non-personal data frameworks[126] also seem to put forth a significant burden on the e-commerce entities. Right from the heavy registration requirements as data businesses to obligations cast upon if the e-commerce entity is a data custodian or data processor, there might be unnecessary burden created on the entities. For example, data custodians have to share appropriate NPD when data requests are made for defined data sharing purposes. Further, the custodians have the obligation of responsible data stewardship and a *duty of care* to the concerned community. This framework also put forth requirements to respond to specific, targeted data sharing requests for legitimate purposes (sovereign, public good, etc.) unless it involves access to trade secrets, proprietary information (regarding internal processes, employees, productivity) or unless it is likely to violate privacy of individuals, groups, or communities. Additionally, entities also have to implement an architecture that allows for such data requests, anonymisation of data, etc. This is a major requirement which creates a mandatory obligation on data businesses at a certain threshold to rewrite their architecture to allow such data sharing.

[125]Report by Committee of Experts on Non-Personal Data Governance Framework. (2020). Ministry of Electronics & Information Technology. https://static.mygov.in/rest/s3fs-public/mygov_160922880751553221.pdf

[126]*Id.*

C. Competition Law

This chapter provides an overview of the Competition Act, 2002 ("**Competition Act**") and its applicability to the ecommerce sector in India. The Competition Act vests the power in the Competition Commission of India (CCI) to promote competition in India.

Broadly, the Competition Act prohibits anti-competitive agreements, abuse of dominance and combinations that cause appreciable adverse effect on competition ('**AAEC**') in India. The discussion in the following sections would set out each of these in greater detail.

(i) Anti-Competitive Agreements

Section 3 of the Competition Act states that any agreement which causes or is likely to cause AAEC in India is anti-competitive.[127]

a. Horizontal Agreements

Section 3(3) of the Competition Act governs horizontal or agreements between competitors. This section provides that agreements or a 'practice carried' on by enterprises or persons (including cartels) engaged in trade of identical or similar products are presumed to have AAEC in India if they: -

- Directly or indirectly fix purchase or sale prices;
- Limit or control production, supply, markets, technical development, investments or provision of services;
- Result in sharing markets or sources of production or provision of services;
- Indulge in bid-rigging or collusive bidding.

Horizontal agreements relating to activities referred to under Section 3 (3) above create a rebuttable presumption that they have an AAEC within India. The Supreme Court of India in *Sodhi Transport Co. v. State of U.P.*[128] has interpreted '*shall be presumed' as a presumption and not evidence itself, but merely indicative on whom burden of proof lies*. Firms can rebut this presumption by either demonstrating that an 'agreement'[129] in terms of the categories identified under Section 3(3) of the Competition Act do not exist or by showing that the agreement is pro-competitive. Note that the joint venture defence under the proviso to this section allows efficiency enhancing joint venture between competing firms.

---

[127]Section 3 (1) of the Competition Act prohibits any agreement with respect to "production, supply, distribution, storage, and acquisition or control of goods or services which causes or is likely to cause an appreciable adverse effect on competition within India". Section 19 (3) of the Act specifies certain factors for determining AAEC under Section 3:
(a) creation of barriers to new entrants in the market;
(b) driving existing competitors out of the market;
(c) foreclosure of competition by hindering entry into the market;
(d) accrual of benefits to consumers;
(e) improvements in production or distribution of goods or provision of services;
(f) promotion of technical, scientific and economic development by means of production or distribution of goods or provision of services.

[128]AIR 1986 SC 1099.

[129]Agreement is defined under Section 2(b) of the Competition Act in the following manner: "agreement" includes any arrangement or understanding or action in concert,— (i) whether or not, such arrangement, understanding or action is formal or in writing; or (ii) whether or not such arrangement, understanding or action is intended to be enforceable by legal proceedings.

Penalty for contravening Section 3(3) can go up to 10% of the average of the past three years relevant turnover of the company. In case of a cartel, the CCI can impose a higher fine based on the proviso where it can impose a penalty based on three times the profits from the cartel or up to 10% of the relevant turnover during the duration of the cartel. In addition to penalties, the CCI can impose both behavioural and structural remedies.

b. Vertical Agreements

Vertical agreements are assessed under Section 3(4) of the Competition Act[130] and includes agreements between suppliers and producers at different levels of the production chain. Section 3(4) provides the following inclusive list of vertical agreements:

- Exclusive agreements;
- Resale price maintenance;
- Refusal to deal; and
- Tying arrangements.

Vertical agreements are not per se prohibited under the Competition Act. Section 3(4) only prohibits vertical agreements that cause AAEC in India. Once a vertical agreement is classified as falling under any of the buckets listed between (a) to (d), the CCI undertakes a rule of reason analysis to balance the pro-competitive effect against any anti-competitive effect. Section 19(3) of the Competition Act lists the balancing factors that the CCI relies on to conduct an AAEC analysis. As outlined above, procompetitive effects include benefits to consumers or efficiencies from the arrangement. Anti-competitive effects include barriers to entry and foreclosure of rivals. In addition to the above, the CCI has held that parties must have substantial market power in their respective market segments (typically above 30%) for the vertical agreement to cause AAEC in India.[131]

Penalty for contravening Section 3(4) can go up to 10% of the average of the past three years relevant turnover of the company. In addition to penalties, the CCI can impose both behavioural and structural remedies.

[130]Section 3(4) of the Competition Act: Any agreement amongst enterprises or persons at different stages or levels of the production chain in different markets, in respect of production, supply, distribution, storage, sale or price of, or trade in goods or provision of services, including—(a) tie-in arrangement; (b) exclusive supply agreement; (c) exclusive distribution agreement; (d) refusal to deal; (e) resale price maintenance, shall be an agreement in contravention of sub-section (1) if such agreement causes or is likely to cause an appreciable adverse effect on competition in India. Explanation.—For the purposes of this sub-section,— (a) "tie-in arrangement" includes any agreement requiring a purchaser of goods, as a condition of such purchase, to purchase some other goods; (b) "exclusive supply agreement" includes any agreement restricting in any manner the purchaser in the course of his trade from acquiring or otherwise dealing in any goods other than those of the seller or any other person; (c) "exclusive distribution agreement" includes any agreement to limit, restrict or withhold the output or supply of any goods or allocate any area or market for the disposal or sale of the goods; (d) "refusal to deal" includes any agreement which restricts, or is likely to restrict, by any method the persons or classes of persons to whom goods are sold or from whom goods are bought; (e) "resale price maintenance" includes any agreement to sell goods on condition that the prices to be charged on the resale by the purchaser shall be the prices stipulated by the seller unless it is clearly stated that prices lower than those prices may be charged.

[131]*In Re: M/S K.C. Marketing and OPPO Mobiles MU Private Limited*, Case No. 34 of 2018 (Competition Commission of India). https://www.cci.gov.in/sites/default/files/34-of-2018.pdf

(ii) Abuse of Dominance

Section 4 of the Competition Act, 2002 governs unilateral conduct and prohibits any enterprise from abusing its dominant position in a relevant market. The abuse of dominance analysis starts with the determination of relevant markets. Once the relevant market has been determined, the CCI's next task is to establish whether the enterprise enjoys a dominant position within the relevant market. The Competition Act, 2002 does not prohibit the mere possession of dominance that could have been achieved through superior economic performance, innovation or pure accident but rather only its abuse.[132] Once dominance is established within a relevant market, the CCI must demonstrate that the conduct being investigated falls under one of the sub-categories of Section 4. Each of these steps are discussed in detail below.

a. Relevant Market

The Competition Act, 2002 defines the relevant market as '*with reference to the relevant product market or the relevant geographic market or with reference to both the markets*'.[133] The relevant geographic market is defined as '*a market comprising the area in which the conditions of competition for supply of goods or provision of services or demand of goods or services are distinctly homogeneous and can be distinguished from the conditions prevailing in the neighbouring areas*.'[134] [135]

The relevant product market is defined as '*a market comprising all those products or services which are regarded as interchangeable or substitutable by the consumer, by reason of characteristics of the products or services, their prices and intended use*'.[61] [136]

b. Dominance

The term '*dominant position*' has been defined in the Competition Act, 2002 as '*a position of strength, enjoyed by an enterprise, in the relevant market, in India, which enables it to operate independently of competitive forces prevailing in the relevant market; or affect its competitors or consumers or the relevant market in its favour'.*

---

[132]Section 19 (7), The Competition Act, 2002.

[133]Section 2 (r), The Competition Act, 2002.

[134]Section 2 (r), The Competition Act, 2002.

[135]The Competition Act further provides that the CCI shall determine the relevant geographic market having due regard to all or any of the following factors#:

(a) regulatory trade barriers;
(b) local specification requirements;
(c) national procurement policies;
(d) adequate distribution facilities;
(e) transport costs;
(f) Language;
(g) consumer preferences;
(h) need for secure or regular supplies or rapid after-sales services.

[136]The Competition Act provides that the CCI shall determine the relevant product market having due regard to all or any of the following factors:

(a) physical characteristics or end-use of goods
(b) price of goods or service
(c) consumer preferences
(d) exclusion of in-house production
(e) existence of specialized producers
(f) classification of industrial products

The Competition Act sets out following factors which the CCI takes into account to establish the dominant position of an enterprise[137]:

- market share of the enterprise;
- size and resources of the enterprise;
- size and importance of the competitors;
- economic power of the enterprise including commercial advantages over competitors;
- vertical integration of the enterprises or sale or service network of such enterprises;
- dependence of consumers on the enterprise;
- monopoly or dominant position whether acquired as a result of any statute or by virtue of being a Government company or a public sector undertaking or otherwise;
- entry barriers including barriers such as regulatory barriers, financial risk, high capital cost of entry, marketing entry barriers, technical entry barriers, economies of scale, high cost of substitutable goods or service for consumers;
- countervailing buying power;
- market structure and size of market;
- social obligations and social costs;
- relative advantage, by way of the contribution to the economic development, by the enterprise enjoying a dominant position having or likely to have an appreciable adverse effect on competition;
  any other factor which the Commission may consider relevant for the inquiry.

c. Abuse

Dominance *per se* is not bad. Section 4 (2) sets out the following list of activities that shall be deemed abuse of dominant position if practised by a dominant enterprise.

- anti-competitive practices of imposing unfair or discriminatory trading conditions or prices or predatory prices,
- limiting the supply of goods or services, or a market or technical or scientific development, denying market access,
- imposing supplementary obligations having no connection with the subject of the contract, or
- using dominance in one market to enter into or protect another relevant market.

Penalty of contravening Section 4 can go up to 10% of the average of the past three years relevant turnover of the company. In addition to penalties, the CCI can impose both behavioural and structural remedies.

[137]Section 19(4), The Competition Act, 2002.

(iii) Merger Control

Mergers and acquisitions that cross the jurisdictional thresholds set out under Section 5 of the Competition and that do not qualify for any exemptions are considered combinations. Combinations require mandatory CCI approval prior to consummation. Combinations are subject to the standstill provisions of the Competition Act and parties have a suspensory obligation on implementing the combination prior to CCI approval.

(iv) Competition law enforcement in the e-commerce sector

The CCI has been actively watching the e-commerce space. To begin with, the CCI conducted a market study in the e-commerce sector ('Market Study') in 2020.[138] In the Market Study, it was noted that improving transparency would reduce information asymmetry with respect to search ranking criteria, collection, use and sharing of data and review and rating mechanisms.[139]

The business model of the e-commerce marketplace has presented certain novel questions before the CCI. For instance, while defining relevant markets, the CCI has considered whether online and offline markets should be considered separate. While dealing with a complaint against Flipkart, the CCI itself has acknowledged that from a consumer perspective, the line between online and offline distribution channels can be blurry at times.[140] While assessing markets from the supply side, the CCI has focussed on cost effectiveness and scalability resulting from network effects to declare whether offline and online are two separate markets.[141]

The CCI has also been watching pricing and listing of products on e-commerce platforms. Notably, while assessing claims of unfair/discriminatory product listing against Flipkart, the CCI ordered a closure order after noting that Flipkart devised the arrangement of its search results on an objective criterion.[142]

In one of the earliest cases, the e-commerce company, Snapdeal, complained to the CCI that Kaff (a manufacturer and seller of kitchen appliances) imposed a resale price on Snapdeal in violation of Section 3(4) of the Competition Act.[143] One of the key questions before the CCI in the Snapdeal case was whether sale of products on the e-commerce website can be considered as a 'resale'. The confusion stemmed from the fact that e-commerce companies cannot be considered as conventional distributors. The CCI held that sellers and e-commerce platforms are vertically integrated in terms of Section 3(4) of the Competition Act because the e-commerce website provides value added services like, grievance redressal opportunities. From the CCI's perspective, there was a corollary between distributors and e-commerce companies and therefore, sale through the online platform could be construed as resale. The CCI dismissed the complaint after an inquiry revealed that even though the manufacturer tried to control the discounts offered by Snapdeal on its website, there was no evidence of adverse impact on intra-brand competition.

The European Commission recently started an investigation against Amazon examining if the use of seller data by them for product listing distorts competition.[144]

---

[138]CCI Market Study Report, *supra* note 14.

[139]*Id.*

[140]*All India Vendors Association v Flipkart India Private Limited*, Case No. 20 of 2018 (Competition Commission of India). https://www.cci.gov.in/sites/default/files/40-of-2019.pdf

[141]*Id.*

[142]*Id.*

[143]*Jasper Infotech v Kaff Appliances,* Case No. 61 of 2014 (Competition Commission of India). https://www.cci.gov.in/sites/default/files/61-of-2014.pdf

[144]European Commission. (2019, July 17). *Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon* [Press Release]. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4291

The consequences for non-compliance under the Competition Act are quite high. The e-commerce sector is still at a nascent stage in India and the CCI is watching this space. As players come up with innovative business models, transparency and objectivity is key.

D. Taxation Laws

(i) Withholding / Collection Obligations under Income Tax Act, 1961

The Finance Act, 2020 introduced Section 194-O in the Income Tax Act, 1961 ("**ITA**") with the objective of deepening and widening the tax base.[145] Section 194-O casts an obligation on an e-commerce operator to deduct tax at source for facilitating any sale of goods or provision of services by an e-commerce participant. For the purpose of section 194-O, e-commerce has been defined as *supply of goods or services or both, including digital products, over digital or electronic networks. Further, e-commerce operator has been defined as a person who owns, operates or manages digital or electronic facility or platform for electronic commerce.*

Issues with Section 194-O

Even where the consideration does not flow through the e-commerce operator (for example, where products are merely listed on the e-commerce portal and buyer purchases from the seller directly), Section 194-O requires it to withhold taxes. This vague requirement may also apply where the e-commerce operator may not have visibility or control over the entire transaction, and further the e-commerce operator may not have any relationship with the buyers to enforce compliance of withholding. For instance, if the platform is a C2C site that enables product discovery and individuals may then in person decide to annul or complete the transaction or vary the price, the platform would have no knowledge. Nevertheless, the terms used are broad enough to potentially capture such situations as the platform may be viewed as 'facilitating´ the sale. One of the e-commerce operators has raised this issue before the Calcutta High Court and the matter is pending to be heard.[146] The government has issued limited use cases in the past to exempt certain businesses under this section such as transactions in commodities markets, insurance payment gateways[147] and very recently e-auction websites, however there is a need for a broader and reasonable approach to exempt businesses which do not oversee such transactions.[148]

Further, there are certain e-commerce models or aggregators where e-commerce operators may not be earning any commission from the sellers/buyers. Hence, levying TDS obligation on such e-commerce models impacts the working capital requirement and creates administrative issues. It is pertinent to note that even GST law also imposes a tax collection at source obligation on the e-commerce operators, however the obligation is limited only when the consideration is "collected" by the e-commerce operator.

The e-commerce industry has dynamic business models. There is a possibility that multiple e-commerce operators are involved in a supply chain. For example, in hotel booking platforms, an e-commerce operator (A Co.) may merely list the products of various other online sellers or e-commerce operators (B Co.). Hence,

[145]Memorandum to Finance Bill, 2021

[146]*Mjunction Services Ltd and Anr. v Union of India and Ors.* WPO No. 441 of 2021.

[147]Central Board of Direct Taxes. (2020, September 29). Guidelines under section 194-0 (4) and section 206C (1-1) of the Income-tax Act, 1961. Circular No. 17 of 2020. https://www.incometaxindia.gov.in/Communications/Circular/Circular_17_2020.pdf

[148]Central Board of Direct Taxes. (2021, November 25). Guidelines under sub-section (4) of section 194-0, sub-section (3) of section 194Q and sub- section (I-I) of section 206C of the Income-tax Act. Circular No. 20 of 2021. https://www.incometaxindia.gov.in/news/circular-20-2021.pdf

for the customer A Co.'s platform will only be a marketplace and the actual sale may happen on the B Co.'s platform. In such cases, there is a concern whether both A Co. and B Co. will be liable to withhold tax under Section 194-O.[149]

Section 194-O(2) provides that no deduction is required where the e-commerce participant (seller) is an individual or HUF, provided that gross amount of sale or services provided during a year through the e-commerce platform does not exceed INR five lakhs and the e-commerce participant has provided PAN or Aadhar. Hence, if the annual consideration exceeds INR five lakhs, then the e-commerce operator will be required to withhold on the whole sum and not merely the sum which exceeds INR five lakhs. This is quite an onerous obligation, as the e-commerce operator will need to forecast annual sales of the participant at the start of the year, and withhold the consideration amount from the first transaction itself.

(ii) Requirements Under GST

Section 2(44) of the CGST Act, 2017 defines e-commerce operator as '*any person who owns, Operators or manages digital or electronic facility or platform electronic commerce*'. Per Section 52 of the CGST Act, every e-commerce operator has to collect TCS not exceeding 1% of the net value of the taxable supplies, made through the operator and, where the consideration with respect to such supplies is to be collected by such operator. Further, Section 24(x) of the CGST Act mandates every e-commerce operator to obtain the GST registration in each state in case their suppliers are from different states. Similarly, per section 24(ix) of CGST Act, sellers operating on the e-commerce platform also have to get registered under GST irrespective of the turnover threshold.

There has been disparity in terms of tax regime for online and offline retailing which is a cause of concern. Compared to the offline retailing, where exemption to registration under GST has been provided for businesses having intra state sales under INR 40 Lakh (for goods) and INR 20 lakhs (for services), online retailing does not have any threshold. Similarly, a supplier selling goods through an e-commerce platform does not have the option to take the benefits of composition schemes that are available to offline retailers, as section 10(2)(d) of the CGST Act carves out an exception for such suppliers. A number of suppliers sell offline as well as online. Hence, a small/medium sized supplier who would be otherwise exempt from registration or eligible for composition scheme, may be put at a competitive disadvantage merely because of selling online, since selling online requires such sellers to comply with onerous registration and compliance obligations.[150] This disincentives the size of the online market for trade and impacts smaller businesses disproportionately.

(iii) Equalisation Levy

The scope of the Equalisation Levy was significantly increased by the Finance Act 2020 (**"E-commerce EL"**) and it was made applicable on consideration received by a non-resident e-commerce operator from any e-commerce supply of goods or provision of services. The e-commerce operator is defined as '*a non-resident who owns, operates or manages a digital or electronic facility or platform for online sale of goods or online provision of services or both.*'

[149]The National Association of Software and Service Companies. (2021). *NASSCOM's suggestions for Union Budget 2022-23*.https://community.nasscom.in/communities/policy-advocacy/nasscoms-suggestions-union-budget-2022-23#

[150]The National Association of Software and Service Companies. (2021). GST: *Submission highlighting key GST issues faced by e-commerce industry*. https://community.nasscom.in/communities/policy-advocacy/gst-submission-highlighting-key-gst-issues-faced-e-commerce-industry

The E-commerce EL has been defined very broadly and given that certain key terms such as ‘online sale of goods’, ‘online provision of service’, the words ‘online sale of goods’ and ‘online sale of services’ have now been defined very broadly to include any supply of goods or provision of services, partly or wholly conducted online. Hence, even if only a part of the transaction occurs online, it could be subject to E-commerce EL. From a policy perspective, this is problematic as it blurs the line between where e-commerce ends and where non-e-commerce trading begins. Instead of e-commerce relating to sales conducted over the internet for instance, any sale that is even partly conducted online may be covered. It raises questions as to whether for instance services of an architect in terms of providing a building plan becomes an online service for E-commerce EL only because it is sent over email or a private portal.

The scope of the consideration has also been clarified to include consideration for sale of goods/provision of services irrespective of whether the e-commerce operator owns the goods/provides or facilitates the services. This has the potential to have a significant impact on marketplaces operated by the e-commerce operators since the E-commerce EL is likely to apply on the total value of the sale of goods or provision of services facilitated by them as opposed to being charged only on any commission earned by the platform. Further, due to amendments, if an e-commerce operator is enabling the supply of goods or services by Indian resident sellers, then the whole transaction is effectively exempt, which is contrary to the original intent of taxing the commission earned by such e-commerce operators. Further, the rationale for such a move is based on the assumption that income earned by the Indian sellers is already taxed in India (and therefore should not be subject to EL), however this may not be always true since Indian companies can claim loss carry forward and do not pay taxes unless they are profitable, whereas EL applies irrespective of actual profitability.

The Dialogue™
INFORM ENGAGE IDEATE

Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

https://thedialogue.co

https://www.nishithdesai.com/