E-COMMERCE ISSUES AT THE WTO DISCUSSIONS AND IN INDIA

RIS
Research and Information System
for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

E-Commerce Issues at the WTO Discussions and in India

Arun S. Nair

RIS
Research and Information System
for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

ISBN : 81-7122-155-6

Published in March 2020 by:

RIS
Research and Information System for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

Core IV–B, Fourth Floor, India Habitat Centre
Lodhi Road, New Delhi–110 003, India
Ph.: +91–11–24682177–80, Fax: +91–11–24682173–74
E–mail: dgoffice@ris.org.in
Website: www.ris.org.in

Contents

Preface

Prof. Sachin Chaturvedi
Director General, RIS

Trade is an important pillar of the research programme of RIS. The institute has undertaken a number of research studies on various aspects of bilateral, regional and multilateral trade issues. As is well known, currently, Digital Technology has acquired the center stage in the global trade discourse. It is manifested in different ways such as the proposal on permanent moratorium on electronic transmission and constitution of Plurilateral Group on e-commerce in the WTO Ministerial Meeting at Buenos Aires.

Recently, India also came out with a draft e-commerce Policy in order to create a regulatory and developmental profile in a rapidly rising sector. The role of data and the related opportunities and challenges continue to engage our attention. Thus, there are several issues in the realm of digital technology, which need the attention of policy makers and experts globally.

RIS took the initiative of organising a seminar on "Digital Economy, e-commerce and the WTO" in June 2019 at New Delhi to discuss various issues related to Moratorium on Electronic Transmission; Data Opportunities and Challenges; and India's Draft e-commerce Policy. Apart from these, there are also issues related to a lack of preparedness of developing countries to take full advantage of opportunities inherent in e-commerce.

It is in this context that we have brought out the present report on *E-commerce Issues at the WTO Discussions and in India* by Mr Arun S. Nair. Earlier, a brief version of the same was discussed at the seminar on "Digital Economy, e-commerce and the WTO" organised by RIS in June 2019. I am sure the Report would be found interesting and useful by all stakeholders.

I also take this opportunity to thank Ambassador (Dr) Mohan Kumar, Chairman, RIS; Mr Rajeev Kher, Distinguished Fellow, RIS; and Prof. Manmohan Agarwal, Adjunct Senior Fellow, RIS for their valuable comments and suggestions on the contents of the Report.

Sachin Chaturvedi

Abbreviations and Acronyms

APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of South East Asian Nations
AVIA	Asia Video Industry Association
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-to-Government
BEPS	Base Erosion and Profit Shifting
BHIM	Bharat Interface for Money
BSA	The Software Alliance
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
C2G	Consumer-to-Government
CAD	Computer-Aided Design
CAIT	Confederation of All India Traders
CBPR	Cross-Border Privacy Rules
CCI	Competition Commission of India
CIGI	Centre for International Governance Innovation
CPPPs	Consumer Privacy Protection Principles
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
DFFT	Data Free Flow with Trust
DFQF	Duty Free and Quota Free
ECIPE	European Center for International Political Economy
EU	European Union
eWTP	Electronic World Trade Platform
FDI	Foreign Direct Investment
FIPPs	Fair Information Practice Principles
FTA	Free Trade Agreement
G2B	Government-to-Business
G2G	Government-to-Government
GATT	General Agreement on Tariffs and Trade
GATS	General Agreement on Trade in Services
GDPR	General Data Protection Regulations
GeM	Government e-Marketplace
GST	Goods and Services Tax
GSC	Global Services Coalition

GVC	Global Value Chain
HEW	Health, Education and Welfare (U.S. Department)
HUF	Hindu Undivided Family
ICC	International Chamber of Commerce
ICT	Information and Communications Technology
IPR	Intellectual Property Rights
IRDAI	Insurance Regulatory and Development Authority of India
IT	Information Technology
ITA	Information Technology Agreement
ITC	International Trade Centre
ITIF	Information Technology and Innovation Foundation
LDC	Least Developed Countries
MC11	11th Ministerial Conference
M2M	Machine-to-Machine
MIKTA	Mexico, Indonesia, Korea, Turkey and Australia
MNE	Multinational Enterprises
MSME	Micro, Small and Medium-sized Enterprises
NASSCOM	National Association of Software and Services Companies
NTIA	National Telecommunications and Information Administration
NVC	Non-Violation (and Situation) Complaints
OCC	Online Curated Content
OECD	Organisation for Economic Co-operation and Development
OWINFS	Our World is Not for Sale
PAN	Permanent Account Number
PDP	Personal Data Protection
RBI	Reserve Bank of India
RIPD	Ibero-American Data Protection Network
RTA	Regional Trade Agreement
SDG	Sustainable Development Goals
TDS	Tax Deducted at Source
TPP	Trans-Pacific Partnership
TRIPS	Trade-Related aspects of Intellectual Property rights agreement
UNCTAD	United Nations Conference on Trade and Development
USD	US Dollar
USMCA	United States-Mexico-Canada Agreement
USISPF	US-India Strategic Partnership Forum
VAT	Value Added Tax
WTO	World Trade Organization

I

Introduction

Discussions on whether e-commerce should be subjected to multilateral negotiations and rule-making have gathered momentum (WTO, 2019a), though the views are somewhat polarised on account of concerns regarding privacy and security as well as due to the implications of free cross-border data flows on the one hand and data-localisation measures on the other (WTO, 2019b). The divergence of positions of countries on the issue is regardless of the general robust growth in global e-commerce sales and cross-border Business-to-Consumer (B2C) sales. This growth is thanks to greater business innovations attracting more consumers towards online shopping – a process that has led to employment generation, greater export opportunities, consumer empowerment in terms of better choices at lower prices as well as development in many economies across the world (UNCTAD, 2019a; WTO, 2019b). However, there are concerns over the efforts toward global rule making on e-commerce. These apprehensions are due to the digital divide as well as inadequate capacity and preparedness of developing countries to either participate effectively in such multilateral negotiations or gain substantially from cross-border e-commerce. There are worries about the domination of the digital trade by a few big multinational companies and rich countries with advanced infrastructure, technology, standards and technical regulations as well as the possibility of them consolidating their position by exerting undue influence over weak countries and small firms through the World Trade Organization (WTO) rule-making process (OWINFS, 2019). This kind of domination - by a few advanced nations and large corporate entities through various means of data collection from nations that do not have well-developed data regimes and strong capacity to comprehend the consequences of parting with data sans any consideration or conditions - has been perceived in some quarters as 'digital colonialism'. Many of the dominated countries belong to the developing world, and it is important for them to consider a holistic approach - covering education, research, skill development and capacity building - through state-funding to protect their digital sovereignty and address digital inequalities (Pinto, 2018).

UNCTAD data shows a 12 per cent growth in online shoppers in 2017 to 1.3 billion people (or a quarter of the global population). In 2017, the global e-commerce sales - comprising Business-

to-Business (B2B) and B2C sales - were USD 29.37 trillion, registering a 13 per cent year-on-year growth. The B2B sales were around 87 per cent of the global e-commerce sales (or USD 25.52 trillion), while the B2C sales accounted for the remaining around 13 per cent (or USD 3.85 trillion). Cross-border B2C e-commerce sales accounted for USD 412 billion, or close to 11 per cent of B2C e-commerce sales. This also meant that *cross-border B2C e-commerce sales were only a minuscule 1.4 per cent of the global e-commerce sales. However, cross-border B2C e-commerce sales have been growing - as their share of 11 per cent of B2C e-commerce sales in 2017 was up from 7 per cent in 2016.* Developed countries dominate the sector in terms of various parameters including e-commerce sales and cross border B2C sales (UNCTAD, 2019a). B2C e-commerce and cross-border B2C e-commerce activities tend to get greater attention than its B2B counterpart, thanks to the availability of more estimates than the latter.[1]

Digital trade benefits producers and traders, including the Micro, Small and Medium Enterprises (MSMEs), as it lowers costs and provides them the opportunity to integrate deeply with Global Value Chains as well as to easily access markets overseas. It also gives greater choice of products and services to consumers. However, since the growth of the sector depends - to a large extent - on cross-border data flows, restrictions to such flows have emerged as a major challenge. Given the global dimensions and implications of this challenge, efforts are on to address it at the international level through consensus between countries on the various related issues. This includes whether the regulations should enable free flow of data across borders without any riders or make cross-border data flow conditional on certain safeguards. Other fundamental elements include the differences in definitions of digital trade and the difficulties in measuring digital trade. However, according to an OECD study, there is a 'growing consensus' that digital trade includes 'digitally-enabled transactions of trade in goods and services that can either be digitally or physically delivered, and that involve consumers, firms, and governments' (López González and Jouanjean, 2017).

Plurilateral Initiative

The topic of global e-commerce rules gained impetus at the WTO-level when a group comprising 71 developed and developing countries, contributing to about 77 per cent of global trade, jointly proposed at the 2017 Ministerial Conference at Buenos Aires to start "exploratory work together toward future WTO negotiations on trade-related aspects of e-commerce" with a view to ensure that consumers and businesses around the world gain more from e-commerce. The proponents of this proposal have kept the initiative open for all WTO Members to join, without prejudice to their positions on future talks. Due recognition was accorded to the WTO's role in promoting 'open, transparent, non-discriminatory and predictable' regulatory environments in facilitating e-commerce. The proponents said the talks would be held without prejudice to existing WTO agreements and mandates as well. They have recognised not just the opportunities that e-commerce will provide to the developing nations, especially the Least Developed Countries (LDCs), and MSMEs, but also the specific challenges that the developing world and MSMEs are facing (WTO, 2017a). They are concerned about the various 'hindrances' to e-commerce trade. These obstacles, according to them, are in the form of regulatory barriers, including payment systems-related and the norms preventing or restricting free-flow of data across borders.

Ramifications

The issues related to e-commerce have their implications and ramifications beyond trade and the WTO. This report, therefore, reviews

the developments at the WTO-level discussions and at the bilateral and regional levels in one chapter and then at the national level (the scenario in India was chosen for this study as it is among the world's fastest growing e-commerce markets) in another. The report recognises the centrality of privacy, security and trust in any e-commerce-related discussion and has a chapter dedicated to those aspects. Data now has become a very precious, if not the most valuable, commodity. This trend is backed by the remarkable growth being registered by the e-commerce sector. Countries, companies, organisations and even individuals are focusing on effective protection of their 'sensitive' data (including confidential, community and personal data). However, they are also considering ways to sensibly leverage 'non-sensitive' data. Governments are coming up with various methods to levy taxes and duties on digital products and services to boost their revenues in order to address the developmental needs and challenges. They are also looking at strengthening data-related regulatory cooperation to safeguard common interests. Developing countries have the option of converting non-sensitive data into a bargaining chip at trade negotiations by asking for transfer of the latest technology in return from the developed nations. However, developing nations would need to negotiate and ensure that provisions regarding access to source code (a type of trade secret that is the original version of a computer programme used to make an executable programme) are incorporated in trade pacts as part of transfer of technology requirements where the technology has the source code (Smith, 2017). Taking full advantage of e-commerce opportunities will help nations to narrow inequalities and meet the Sustainable Development Goals (SDG) targets related to sustainable economic growth, gender equality and participation in international trade, as per a recent WTO report on 'mainstreaming trade to attain the SDGs'. However, the countries engaged in e-commerce discussions at the WTO should also pay heed to the words of caution in the report, which states that "any multilateral action on e-commerce would need to be accompanied by significant support to improve digital connectivity, capacity and infrastructure in those countries that need it the most, in line with infrastructure targets under SDG 9 ('build resilient infrastructure, promote inclusive and sustainable industrialisation and foster innovation')" (WTO, 2018a).

Endnote

1. According to an UNCTAD-commissioned study, 'data on B2B e-commerce are generally scarce' and 'generally, there are many more estimates on B2C than on B2B e-commerce,' although 'B2B e-commerce is likely to be much more significant for international trade in both goods and services.' It stated: "There are no official national data on the value of overseas e-commerce sales broken down by B2B or B2C. Despite the paucity of data, several organisations have made cross-border B2C estimates, based on consumer surveys or some assumed ratio between users that have purchased abroad and the total value of their purchases" (UNCTAD, 2016).

II

Centrality of Privacy, Security and Trust

E-commerce, as per the WTO, is defined as the "production, distribution, marketing, sale or delivery of goods and services by electronic means" and includes such transactions that happen between 'enterprises, households, individuals, governments and other public or private organisations' (WTOa). E-commerce transactions are mainly categorised into Business-to-Business (B2B) and Business-to-Consumer (B2C, which is the most prevalent). However, there are variants including Business-to-Government/Government-to-Business (B2G/G2B, or where the government procures products and services from businesses following a tender process), Consumer-to-Business (C2B, where customers offer their products or services to businesses for a consideration like what is seen on online advertising and survey sites), Consumer-to-Consumer (C2C, including auctions and classifieds on websites), Consumer-to-Government/Government-to-Consumer (C2G/G2C, transactions between government agencies and consumer including those related to payment of electricity and water supply, or health insurance and tax return filing using government websites) and Government-to-Government (G2G, platforms for Governments buying and selling products and services from and to each other) (Rapportrix, 2018; Meghani, 2019).

At the core of all these above-mentioned categories of transactions lies consumer and business entity data. Therefore, minimising or entirely eliminating risks associated with privacy and security aspects of such data has been and will be essential to ensure that e-commerce is conducted in an environment of trust as well as for creating customer loyalty (Wong *et al.*, 2019; Ertemel and Civelek, 2018; Hamidi and Moradi, 2017). Apprehensions over security and privacy are among the major reasons behind consumers shying away from online shopping (Furnell and Karweni, 1999; Udo, 2001; Miyazaki and Fernandez, 2001; Ackerman and Davis Jr, 2003). In this regard, it is important for the e-commerce companies to make investments to develop adequate capacity in technology and human resources to not only securely handle online transactions but also thwart any entity from illegally accessing personal data of their customers. However, e-commerce companies will be prompted to make greater investments in securing transactions and personal data of the consumers in a regulatory regime where such companies are made liable for any breach of privacy or security (Chun, 2019). In order to earn consumer trust, it is also vital for e-commerce companies to ensure a perception of security by bringing out a privacy policy that is strong

and easy-to-understand as well as a system to implement the same (Sarris, 2015).

There is a growing concern among individuals about their online privacy as well as over the perception that governments around the world were not doing enough to protect personal data of the citizens (CIGI-Ipsos, 2019). To address concerns of these kinds in general, several countries have already adopted laws on privacy, consumer protection, e-transactions and cybercrime. Many other nations are in the process of doing so. According to UNCTAD Global Cyberlaw Tracker, of the 194 UNCTAD Member countries, 79 per cent have e-transaction laws, 52 per cent have passed consumer protection laws, 58 per cent nations have privacy laws in place and 72 per cent countries have cybercrime laws. UNCTAD Global Cyberlaw Tracker - 'the first ever global mapping of cyberlaws' - tracks the state of e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime adoption in the 194 UNCTAD member states (UNCTAD, 2019c).

Digital Governance

However, there are varying views on digital governance. A study by O'hara and Hall identified four main emerging views on internet governance as well as the competition among these views to be the winner.

The views include: *(i) 'the Silicon Valley open internet' with transparent standards and with data and software that are 'portable, extensible and interoperable' (even as there are apprehensions that an open internet could be susceptible to hacking and misinformation); (ii) the European Commission model of a 'bourgeois internet' with regulations meant to protect privacy and to curb trolls, but in the process could hamper innovation; (iii) the authoritarian internet model of China and other like-minded nations with an emphasis on 'surveillance and identification technologies' to ensure 'social cohesion and security'; and finally (iv) the commercial model being pushed by the US Republicans that considers online resources as private property meant for monetisation by their owners* (O'hara and Hall, 2018).

The US does not have a comprehensive general law at the federal level on data protection and privacy. It, however, has various sectoral laws at the federal level and legislations at the state level that cover privacy and data protection. Besides, with a view to protect privacy online, the US Federal Trade Commission (the federal agency that enforces federal consumer protection laws including those relating to online privacy and security), which has been looking into online privacy issues since the year 1995, had in 1998 (and later in 2000) detailed the Fair Information Practice Principles (FIPPs). These FIPPs included 'notice' (*the requirement for web sites to provide consumers with clear details of their information practices*), 'choice' (*the requirement for web sites to offer their consumers the choice of how their personal data collected from them during a transaction is used, that is for marketing other products to them and for offering their data to other entities*), 'access' (*ensuring reasonable opportunity for consumers to access their personal data as well as to review, correct inaccuracies or to delete such information*), and 'security *(the requirement of web sites ensure security of the consumers' data*). The Commission had also stated that 'enforcement' through a mechanism of sanctions for any violations would be a part of its online privacy protection measures (Govt. of the US, 2000). The FIPPs are considered to have laid the foundation to privacy laws in the US and in many countries across the world. Their origins are traced to the 'Code of Fair Information Practices' recommended in 1973 by an Advisory Committee in the US Department of Health, Education and Welfare (HEW). This HEW Code of Fair Information Practices (*including access to personal data, data subject's consent for use of personal data, right to correct and amend, and precautions to be taken by*

organisations to prevent misuse of data), along with the subsequent Privacy Protection Study Commission Principles (*ways to minimise intrusiveness including types of data that should not be collected; data subject's right to access their personal data, copy, and correct or amend records to maximise fairness; and specifying obligations with respect to use and disclosure of personal data to ensure legally enforceable expectation of confidentiality*) helped in developing the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data in 1980. These developments led to the drafting of the EU Data Protection Directive Principles (that was approved in October 1995) and subsequently laws in Japan, Canada and other nations as well as the Asia-Pacific Economic Cooperation (APEC) Privacy framework, all on the lines of FIPPs (Cate, 2006). There are also private entities in the US such as TRUSTe providing privacy certifications to help organisations display that they follow responsible data collection and processing practices in line with global and national standards and regulations (TrustArc Inc, 2019).

The General Data Protection Regulation (GDPR) of the EU, in force since May 2018, is arguably the world's strongest data privacy regulation. Article 4 of the GDPR defines 'personal data' as '*any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. The GDPR - which is applicable to entities located within the EU and those situated outside the EU but dealing with EU data subjects – imposes a stringent penalty of up to 4 per cent of annual worldwide turnover or Euros 20 million for violating GDPR. The regulation also covers details aspects such as obtaining consent from the data subject to get their personal data, information that has to be provided where personal data is collected from the data subject, the rights of the data subject including regarding obtaining access to their personal data, as well as the right to rectification and erasure of personal data, the right to restrict processing, and the right to data portability. It also specifies the certain reasonable restrictions to these fundamental rights and freedoms - that is with a view to safeguard national security, defense and public security, among others (EU, 2016). The OECD has also played a significant role in the development of privacy norms. The initial 1980 version of the 'OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data' was updated in 2013 with an aim to bring the focus on risk management for better implementation of privacy protection. The updated version also took into account the global dimension of privacy and emphasised on greater interoperability, in addition to introducing new concepts such as national privacy strategies, privacy management programmes and notification of data security breach. Besides, OECD has its ongoing efforts to further improve privacy protection in the data-driven and digitalising world of today (OECD, 2019a). Other such initiatives include the APEC Privacy Framework and the APEC Cross-Border Privacy Rules (CBPR) System that implements such a framework (APEC, 2019). The CBPR System is a 'voluntary, accountability-based system facilitating privacy-respecting data flows among APEC economies' and its participant economies include Australia, Canada, Chinese Taipei, Japan, Mexico, Singapore, South Korea and the U.S (CBPRS, 2019). In the year 2014, the African Union adopted the Convention on Cyber Security and Personal Data Protection. Out of the 55 AU member countries, only 14 have signed the Convention, while five have ratified it as on June 28, 2019 (AU, 2019). In Latin America, an initiative called the Ibero-American Data Protection Network (RIPD) was launched in 2003 to help develop regulations on personal

data protection. Several Latin American agencies are either members or observers of the network (IPD Network, 2019).

Historical experiences, culture and political changes are among the factors that affect the development as well as implementation of data protection and privacy regulatory frameworks in various countries. There are even nations that are yet to accord privacy the status of a fundamental right (Adelola, Dawson and Batmaz, 2015). Besides, it was seen that though the FIPPs and the subsequent privacy protection guidelines as well as the host of legislations that were enacted in various countries were strong in theory, they were not that effective in practical terms. The business entities were troubled by the legal obligations. On the other hand, though the data subjects received a large number of notices, they either failed to see these notices or did not respond either due to difficulties in understanding the technical language, or due to the lack of clarity or due to the difficulties in exercising their individual choice.

Consumer Privacy Protection

On finding that personal data protection norms and FIPPs were ineffective, an alternative, namely, the 'Consumer Privacy Protection Principles' (CPPPs), was proposed in Cate (2006). These include 'designing data protection laws to: (i) prevent harm to data subjects; (ii) ensure recovery from harms if and when they happen' (*including by making data protection proportional to the chances and severity of the possible harm - by banning the use of data where there is maximum possibility of harm and stepping away from regulation where there is least likelihood of harm*)'; (iii) enact data protection laws that 'maximises both individual and public benefits'; and (iv) 'avoid inconsistency and overlapping with other regulations'. It was recommended that data protection laws should ensure that entities follow 'transparency, honesty and accountability in collection, usage, or transfer personal data'; in addition to making sure that personal data is 'accurate, complete and kept up-to-date'. Besides, it was proposed that the laws should also ensure adequate security of data, and at the same time make sure that the security norms are 'technology-neutral' and do not 'interfere with the development and use of new measures'. It was recommended that the laws should ensure that data users/ collectors are liable only in cases of harm from their 'negligent, willful, or intentional behavior' and not when it 'was not reasonably foreseeable or could not reasonably have been prevented'. It was also suggested that the laws should be drafted in such a manner that it ensures effective enforcement with high compliance rates as well as adequate compensation for victims of personal data misuse (Cate, 2006).

III

Issues at the WTO Discussions

Moratorium on Customs Duties

In 1998, the WTO members came out with a declaration on global e-commerce, agreeing to continue the practice of not imposing customs duties (or a moratorium on customs duties) on e-transmissions in order to boost the e-commerce sector. This moratorium is renewed by the members at every Ministerial Conference, which usually happens every two years. There are demands, especially from the developed countries, to make this temporary moratorium permanent.

The WTO Members have not yet come to an agreement on what all would constitute e-transmissions. However, the major categories of e-transmissions include films, music, video games, software, newspapers and books. There is a notable growth in trading in these items. Among the issues of contention here are whether to apply GATT norms and impose the same customs duties on these products as it is done on imports of such goods in their physical form; or whether the General Agreement on Trade in Services (GATS) provisions need to be applied by treating them as services; or whether the provisions on IPRs need to be applied by considering them as intellectual property.

The idea to impose customs duties on these e-transmissions stems from various reasons. These include the fact that customs duties are a major source of government revenue for developing countries, unlike developed countries. The main implication of the (permanent) moratorium is that customs duty cannot be applied on a digitised product, even though the same product in its physical form attracts a specified customs duty. This would also mean that the moratorium on e-transmissions has an effect of upsetting the prevailing schedule of tariff concessions of WTO Member countries (WTO, 2018b). The schedule of concessions refers to specific tariff concessions and commitments the Members have granted as part of WTO trade negotiation rounds.

Digitisation of Items

Another aspect is the looming prospect of digitisation of a greater number of items, thanks to additive technologies (involving addition of layers of input material to make an item) such as 3D printing and the surge in trade in such digitisable items vis-à-vis the trade in those very items in their physical form. 3D printing can be used for manufacturing products in sectors including automobiles and auto-components, health and medicine (medical devices), aviation (aerospace components), electronics, construction equipment, industrial

machinery, and a host of consumer items such as toys, shoes, textile products, jewellery, furniture and household goods. According to a report by the Dutch banking and financial services giant ING, 50 per cent of manufactured goods will be 3D printed in the year 2060 in a scenario where the current growth of investment in 3D printers continues. However, if investment doubles every five years, the possibility of 50 per cent of manufactured goods being 3D printed could be achieved by 2040 itself. As per the report, such progress in 3D printing of manufactured goods could wipe out around 23 per cent of world trade by 2060 under the first scenario, or 41 per cent by 2040 under the second scenario. However, it should be good news for countries with huge trade deficits, as they would witness their deficits narrowing with such products being 3D printed locally instead of them being imported. Countries such as the U.S., which currently have a high level of import of such products that can soon be 3D printed, would see a greater decline in their deficits once 3D printing takes off in a big way. On the other hand, countries that currently have huge trade surpluses, but are leading exporters of items that can be 3D printed soon, would see their surpluses declining (ING, 2017).

Physical Trading v/s e-transmission

In the physical trading model, on receiving orders from customers, the physical items are transported across the border and the customs department collects the tariffs on these imports. However, in the case of e-commerce/ e-transmission, the seller or designer, on receiving orders from clients, transmit intellectual property-protected Computer-Aided Design (CAD) files across borders through the electronic mode to a local producer in the country. The local producer then manufactures the final item through 3D printing of the CAD files and sends it to the customer using local transport.

The e-transmission model would have many consequences. The ease of the process of transmission of the CAD files, and the increasing use of Big Data analytics to improve efficiency, would substantially reduce global trade in the physical format. There would also be consequences for tax/duty collection. If the seller/designer is operating out of a tax haven and/or is unregistered, it would be difficult to impose taxes due to the challenges involved in getting the details of the transaction and in assessing the value of the product. Besides, due to the moratorium, it would not be possible to impose duties on e-transmissions. On the other hand, with the duty on raw materials being usually lower than that of the finished goods and intermediaries, 3D printing would lead to lesser import tariff revenues. In the services sector such as the hotel and tourism segment, the traditional way of business involves the foreign customer paying the room rent to local hotels, and the local tax authorities collecting taxes from the hotels. However, the e-commerce model involves foreign tourists making their hotel bookings in any country by contacting an e-commerce company located anywhere in the world through its website or an app, and using net-banking or a credit card to pay for the charges. Since the hotel (which may be paying a commission to the e-commerce firm for getting them customers) is not directly involved in this model, the local tax authorities find it tough to get the details of the transaction and impose taxes (WTO, 2018c).

Tariff Revenue Loss

There are apprehensions that a permanent moratorium on customs duties on all digitisable items would subject developing countries to huge tariff revenue loss as compared to developed nations. As developing countries have higher average bound duties than developed countries on digitisable items, they could ensure much greater revenues than their developed country counterparts by levying tariffs on those items. However, incurring massive tariff revenue loss could, in turn, hurt the ability of developing nations to address

many developmental challenges. In December 2016, the WTO Secretariat circulated its report on the fiscal implications of the customs moratorium on e-transmissions. It estimated that the tariff revenue loss is only around USD 756 million. However, the estimate showed that a vast majority (that is, around 92 per cent) of this tariff revenue loss is borne by the developing countries. In February 2019, an UNCTAD study showed that the total potential tariff revenue loss (including physical imports and electronic transmissions) for high income countries (which are WTO Members) due to the moratorium (estimated at the aggregate level in 2017, and using average bound duties) is only USD 289 million. However, as against this, the total potential tariff revenue loss from moratorium for developing countries is to the tune of a whopping USD 10 billion (India's loss is valued at USD 497.2 million).

Digital Taxation

Faced with this situation, several economies (both from the developed and developing world) such as Australia, New Zealand, India, Indonesia and the European Union (EU) brought changes to their laws to raise tax revenues through internal taxes such as Goods and Services Tax (GST – in the case of Australia, New Zealand and India) or Value Added Tax (VAT – imposed by the EU) or customs duties (Indonesia) on imports of intangibles like digital products and remote services, according to the UNCTAD study (UNCTAD, 2019b). France, on 24 July 2019, brought into effect a law on Digital Services Tax (DST) to impose a 3 per cent tax on gross revenues generated from providing "targeted advertising" services and "digital interface" services in France. The tax is applicable only on firms that generate 750 million Euros in global digital revenues and 25 million Euros in French digital revenues. The tax, which is expected to generate 500 million Euros, is temporary in nature and will be applicable till the OECD finds a global solution to the digital taxation issue. The U.S. has alleged that the tax discriminates against American companies. The tax, effective from 1 January 2019, has been termed by the U.S. as one that is retrospective in nature and not consistent with the current principles of taxation (Govt. of France, 2019; Govt. of US, 2019). According to another report, it was found that several other countries are imposing either VAT (Albania, Angola, Belarus, Iceland, Norway, Russia, Saudi Arabia, Serbia, South Africa, South Korea, Switzlerland, Taiwan, Turkey, United Arab Emirates and Quebec in Canada) or GST (Australia) on digital-based businesses, while many more (such as Bangladesh, China, Colombia, Oman, Qatar, Israel, Malaysia, Singapore and Thailand) are considering similar ways of digital taxation. In Japan, there is a consumption tax on digital businesses, while in the US several states have imposed a sales tax on digital products and Software as a Service (SaaS) (Katie, 2019). It was also found that many economies are levying VAT/GST on digital services. These countries include Andorra, Albania, Armenia, Argentina, Australia, Bahamas, Belarus, Brazil, China, Colombia, Egypt, Ghana, Iceland, India, Japan, Kenya, Mexico, Morocco, New Zealand, Norway, Russia, Saudi Arabia, Serbia, Singapore, South Africa, South Korea, Switzerland, Taiwan, Tanzania, Turkey, United Arab Emirates and Uruguay. Some of the e-services include broadcast or satellite services, data telephony services, online voice services, online gambling, web hosting, cloud services, streaming of media and games and subscriptions to membership websites (Avalara, 2019). The counter to the argument on revenue loss comes from the many benefits flowing from digital technologies. The benefits include lower costs of trade, logistics and storage for companies including MSMEs. These technologies also help companies including MSMEs in easily identifying more potential customers in various parts of the world. Digital technologies ensure optimal use of resources, bring greater opportunities for technology transfer as well as enable deeper

integration of firms, especially the MSMEs, with Global Value Chains. They also lead to generation of new products and jobs, and necessitate harmonisation of various regulatory regimes. Though the growth in e-commerce has brought several new opportunities for MSMEs, a complicated indirect tax collection regime would be a barrier for such business entities. Such a regime would increase the cost of compliance. As MSMEs have lesser resources when compared to big companies, they would be more affected in such a case. On the other hand, a simple, consistent and non-discriminatory VAT/GST regime, with easier registration and tax payment processes, would result in a win-win for both the government and the corporate enterprises in general. For instance, Australia has shown that simplicity and consistency in the GST regime could, in fact, garner more revenues and ensure greater compliance due to the ease of compliance (ICC, 2019a).

Meanwhile, concerted efforts are being made at the global level on the issues related to taxation of digital business. It was noted that Multinational Enterprises (MNE) were taking advantage of the global norms that ensure that business entities are not subjected to payment of taxes in two countries (double tax avoidance), and were abusing such rules to avoid paying their 'fair share of taxes'. It was also recognised that the solution to the issue lies in a 'coordinated and multilateral' action. Without such a multilateral solution, the situation could lead to 'uncoordinated unilateral actions' as nations on their own attempt to shield their prevailing tax base and even to widen it. Such 'uncoordinated unilateral actions' carry the risk of complications and undesirable costs for all countries.

Efforts by G20 and OECD

The matter was taken up at the level of the G20 (international platform comprising the world's 20 leading economies), and following a request from the G20, the OECD brought out an Action Plan on Base Erosion and Profit Shifting (BEPS) in 2013. The Action Plan sought to plug the loop holes that were being exploited by the MNEs. The Plan also noted the need to look into the technological advances in the digital economy, which had made it possible for companies to operate in a borderless world and thereby not coming within any specific tax jurisdiction. The Plan aimed to close the loopholes that permitted companies to put away their profits in offshore subsidiaries to avoid them being taxed (OECD, 2019b).

G20 Finance Ministers and Central Bank Governors then came to an agreement to take forward the ambitious work programme that aimed to address the tax challenges arising from digitalisation. They have targeted the year 2020 to arrive at a consensus-based solution on the issues. The work programme has a two-pillar approach – the first is to allocate more taxing rights to market or user jurisdictions so that a country, where a company sells its goods and/or services, can tax such a company, even if the company is based overseas, i.e. in another jurisdiction. As per the second pillar, in case the company somehow manages to book profits in a low/nil tax haven, then the taxing ability of the jurisdiction/country (where the company sells its goods and/or services) would be strengthened by enabling them to levy an agreed global minimum tax rate (G20, 2019a; White and Strupczewski, 2019; and OECD, 2019c). The OECD, on the basis of three competing proposals, brought out a new proposal under the first pillar to ensure that 'large and highly profitable MNEs, including digital companies, pay tax wherever they have significant consumer-facing activities and generate their profits' (*since the focus is not on the physical presence of business entities in the jurisdiction of the user or market, the proposal is considered to benefit countries like India with large number of users as it could lead to greater tax revenues for such nations*). The place of payment

of tax is based on the MNE's sales (*with 'country specific sales thresholds' to ensure that even small economies benefit*). The proposal also has details on the portion of profits that should be taxed (based on a 'new profit allocation rule going beyond the arm's length principle') (OECD, 2019d). The OECD then came up with a public consultation document on the second pillar (also known as the proposal on 'Global Anti-Base Erosion' or 'GloBE'). The aim was to fix a floor on tax rate to make sure that a minimum rate of tax was imposed on the profits of an MNE wherever it is headquartered, and thereby address the outstanding BEPS challenges. The objective here is to deter the MNEs from opting for profit shifting to low/nil tax jurisdictions as well as protect developing nations from yielding to the pressure to come up with 'inefficient tax incentives'. As per the proposal, the minimum rate would be applicable in all cases where the income is currently not taxed at least at the minimum level – that is, the proposed norm would act as a 'top up' to help meet the goal of the minimum rate of tax. The exception to the rule could be in cases of 'income taxed below the minimum rate and benefiting from a harmful preferential regime, which would then be taxed at the higher of the minimum rate or the full domestic rate' (OECD, 2019e).

Data-Related Issues

Data in the digital age has been described as a resource as important as oil in the industrial era due to factors including technologies such as the Internet of Things and the growing digital commerce that uses various data-based services. (Van't Spijker, 2014).

However, there are several examples of oil-rich countries being unable to use the resource to their advantage, and in fact have not been successful even in eradicating poverty. This was due to reasons including lack of a well planned strategy to make efficient use of the inflow of money on account of oil. (Myers, 2005; Schubert, 2006; Peck and Chayes, 2015). Similarly, data-rich countries without proper strategies would find it difficult to benefit from their data resource.

Data, the New Oil?

Data is similar to oil in the sense that both are valuable and essential commodities. While oil was the fuel of the industrial age, data is the same in the information age. Also, both need to be refined in order to be more useful and valuable. However, there are several dissimilarities as well. Data, unlike oil, is not exhaustible and rivalrous (where simultaneous consumption is not possible). Also, unlike oil, it would be difficult to restrict data to a few locations as data can be extracted from multiple sources. In fact, integrating data related to weather, soil and health at a global level could even lead to greater efficiencies and spur innovations. However, placing curbs on such data could have the opposite effect (WTO, 2019b). Economies relying on data and oil function differently. For instance, the challenge with data would be to manage its huge and virtually inexhaustible quantity (unless there is an artificial scarcity owing to various restrictions), while in the case of oil, the challenge would be to manage the shortages. Also, while cost of additional data production would slide to almost nil, the same for production of every extra barrel of oil would be on the rise. (De Wachter, 2015; WTO, 2019b). Besides, while greater export of oil would lead to lesser local consumption, increased data exports would not have to be at the cost of lesser domestic consumption of that same data. In addition, the significant aspect of data-intensive industries is their ability to ensure faster productivity, higher wages and new jobs when compared to industries that are less reliant on data (Mandel, 2017).

Gross Data Product

A study published in Harvard Business Review ranked countries on the basis of what it called the world's top "*gross data product*" producers (See Table 3.1) (Chakravorti *et al.*, 2019).[1]

Table 3.1: World's Top 'Gross Data Product' Producers

Rank	Country
1	U.S
2	U.K
3	China
4	Switzerland
5	South Korea
6	France
7	Canada
8	Sweden
9	Australia
10	Czech Republic
11	Japan
12	New Zealand
13	Germany
14	Spain
15	Ireland
16	Italy
17	Portugal
18	Mexico
19	Argentina
20	Chile
21	Poland
22	Brazil
23	Greece
24	India
25	South Africa
26	Hungary
27	Malaysia
28	Russia
29	Turkey
30	Indonesia

Source: Chakravorti *et al.*, 2019.

Recognising the importance of data produced in their territory, countries have begun considering - or are already taking - data protection measures. These measures include mandatory data localisation, specific norms on data collection, retention, processing and transfer. In this context, many countries have also adopted legislations on privacy, cyber security, e-transactions and consumer protection. However, businesses that rely on data can make the most of the data they collect in terms of profit maximisation and value creation only when the laws allow data to flow freely across borders and with minimum or no restrictions. The European Center for International Political Economy (ECIPE) has come up with a Digital Trade Restrictiveness Index that it claims is the world's first such initiative and measures 64 countries. According to the index, China is the most restricted nation in digital trade, followed by Russia, India, Indonesia and Vietnam, while the most open economies (that is with the least number of trade restrictions) is New Zealand, followed by Iceland, Norway, Ireland and Hong Kong (ECIPE, 2018).

Data Localisation

Data localisation measures are being brought out by governments with a view to retain the data generated in their respective countries within the national borders, and thereby restricting data flows across national borders. The rationale behind such curbs includes ensuring law enforcement, improving surveillance, protecting privacy and boosting the capabilities of local enterprises. Data localisation measures could ensure better protection of the rights of data subjects (as the local law can be applied on data stored within a nation's territory), reduce instances of foreign surveillance and help improve national security measures including those related to counter-terrorism.

Data localisation restriction, in its most extreme form, requires firms to not just store and process data in servers/centres set up within the borders of the country, but also mandate transmission and/or processing of data between servers/centres that are situated only in the national jurisdiction. Transfer of data across borders is allowed only if the firm complies with specific conditions such as meeting certain security safeguards and/

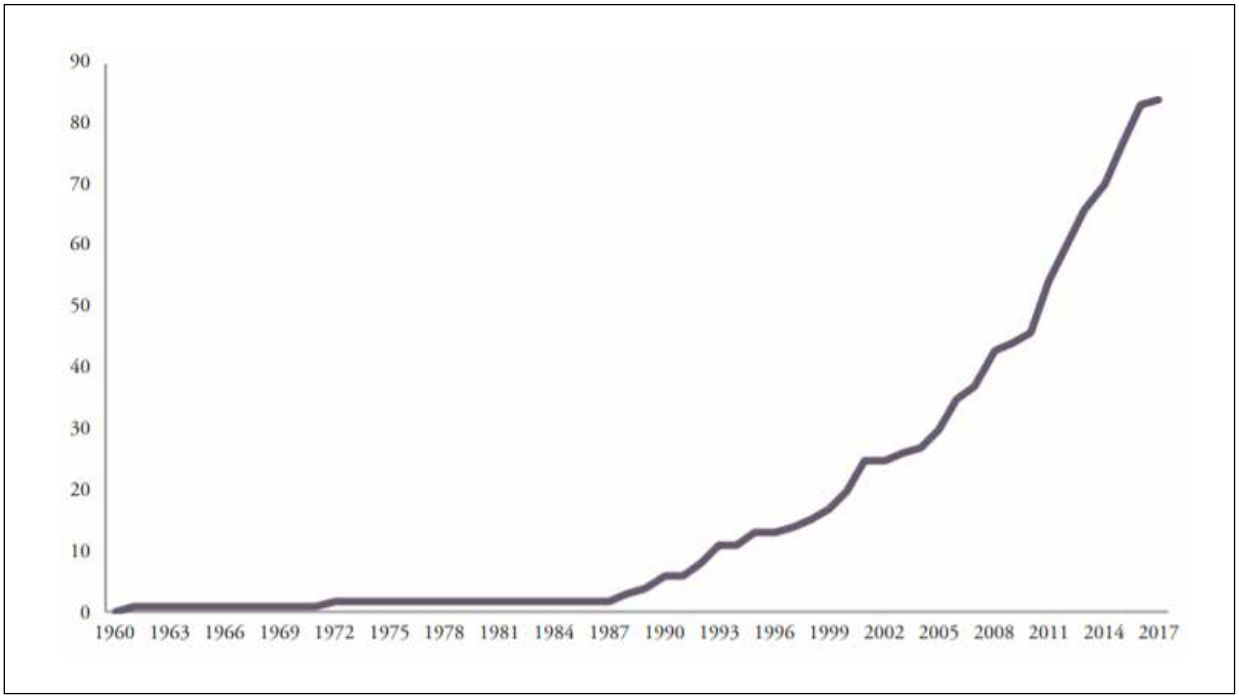
or getting 'informed consent' from customers. Also, the country receiving the data may also have to agree to conditions such as enforcement of privacy or other data protection norms of the country from where the data is sent. It has been argued that mandatory data localisation is a trade restrictive policy as it would lead to increase in costs related to data processing offshore and, in turn, result in lesser foreign investment. Such policies are also found to be barriers to innovation in areas such as cloud computing, Internet of Things, artificial intelligence and Big Data analytics. The worst affected would be the MSMEs as mandatory data localisation could disrupt their integration with Global Value Chains (Bauer, et al., 2014).

As per the ECIPE Digital Trade Estimates database, currently there are around 84 'data localisation' requirements (or measures mandating either local storage of data or imposing conditions for cross-border data transfer) that have been imposed across the 64 countries under review for the Digital Trade Restrictiveness Index. Right from the oldest data localisation measure in 1961 until the year 2000, there were only 19 such measures imposed globally. However, from then on they have registered an exponential growth (See Figure 3.1).

The majority of the measures (42 per cent) included regimes with specific riders for cross-border data transfer. Further, 33 per cent of the measures were in the most restrictive category as they included norms on local processing requirement (regimes mandating the company to use a local server in order to carry out the main processing of the data)/ ban on transfer (countries imposing a ban on transfer do not allow even a copy of the data to be transferred across their borders). The remaining 25 per cent of the measures include local storage requirements (meaning that a copy of the specified data has to be stored within the country) (ECIPE, 2018).

China brought out its first national-level law (Cyber Security Law) in 2017 on data privacy protection and cyber security. It also

Figure 3.1: Overall Data Localisation Measures Across The World (1961-2016)



Source: ECIPE, 2018.

has draft norms, decisions and standards on data security and online information protection, besides laws to protect personal information and consumer rights. China also has data localisation norms specifying that 'personal information' or 'important business data' collected and generated in the operation of 'key (or critical) information infrastructure operators' within its territory shall be stored within its territory itself (Beiten Burkhardt, 2018).

Under the Chinese regulations, cross-border transfer is permitted in cases of "genuine need for reasons of operational necessity", but only after ensuring compliance with the norms related to informed consent of the customer, security assessments and prior regulatory approval. The December 2016 Cyberspace Security Strategy of China defines 'critical (or key) information infrastructure' as "information infrastructure that affects national security, the national economy and people's livelihoods, such that, if data is leaked, damaged or loses its functionality, national security and public interests may be seriously harmed". The sectors and business deemed to be part of 'critical information infrastructure' is exhaustive and include: finance, transportation, energy, social security, sanitation and healthcare, education, water management, public utilities, environmental protection, television stations, radio stations and other news agencies, information networks (including radio, television, telecommunications, the Internet, big data, cloud computing and other large-scale public information network services), scientific research and production in national defence, industrial chemicals and equipment, as well as food and drugs (Bird, 2018). Russia is among the jurisdictions with stringent data localisation laws. The Russian law requires data operators to make sure that collection or use of personal data of Russian citizens is carried out using databases and networks located within the Russian territory. Russia also has specific data localisation norms for the media and financial sectors. Turkey's data localisation rule for e-money institutions and payment services providers mandates them to "keep all the documents and records related to (their activities) for at least ten years within the country, in a secure and accessible manner" (ECIPE, 2018).

Consumer Protection

Also significant here is the discussion on consumer protection measures. With easier and more affordable access to internet now than in the early days of the electronic age, more people across the world are going online to purchase goods and pay for services. However, they face numerous challenges in the process. These include poor and unreliable connectivity, language barriers, unfair commercial practices including misleading advertisements and information regarding goods and services, unreliable traders and service providers, e-payment systems that are not secure, difficulty in getting refunds for substandard products and services, ignorance of various rights as a consumer, in addition to problems with the dispute resolution process including jurisdictional issues. In order to address these issues, it is important to ensure stable internet connection, and bring out a regulatory framework that would protect consumer data and ensure that goods and service providers adhere to quality standards regarding products and services. Besides, the norms should also facilitate greater awareness among consumers regarding their rights, and pave the way for stronger cooperation with regulatory regimes of other countries (UNCTAD, 2017a).

In this regard, it would be important for countries to take note of the WTO's General Agreement on Trade in Services (GATS) while formulating policies. As per the GATS, Member countries can take measures necessary to secure compliance with laws or regulations including those relating to: (i) *the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts*; (ii) *the protection*

of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; and (iii) *safety*." However, in order to ensure free and fair trade, the GATS - through Article XIV (c) - specifies that such measures are "*subject to the requirement that (they) are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services*" (WTOb).

The issues around cross-border data flow would require development of national policies and certainly cooperation with regulatory agencies across the world. However, the argument now is to find ways to move beyond traditional forms of cooperation that were forged through mutual recognition pacts and harmonisation of norms as part of trade agreements.

EU-U.S. Privacy Shield

The world is witnessing new forms of cooperation through quid pro quo arrangements in the field of digital governance. For instance, the U.S. has agreed to ensure protection of privacy of EU citizens to EU standards (including norms on what would constitute adequate level of data protection), in return for transfer of personal data from the EU to the U.S. – that is, to firms certified in the U.S. under the 'EU-U.S. Privacy Shield Framework'. Such cross-border flow of personal data is happening thanks to the Framework incorporating norms on: (i) stringent data protection obligations on the firms that receive personal data from the EU; (ii) assurance to individuals on effective protection of their data and grievance redress; (iii) guarantee by the U.S. government to ensure necessary safeguards and adherence to transparency obligation on accessing data; and (iv) an annual joint review by the U.S. and the EU of the mechanism (EC, 2016). However, countries mulling such an arrangement would necessarily need to build greater institutional capacity to monitor firms and enforce their compliance with the norms of their partner country - like the U.S. would be carrying out through its agencies to ensure that companies comply with the EU privacy norms within America's territorial jurisdiction. However, any unilateral measure to restrict data flows could lead to information asymmetries and increased economic costs. The higher economic costs in such a case would be on account of an adverse impact on exports, particularly related to data-based services, and the difficulties that such curbs cause in achieving economies of scale (Mattoo and Meltzer, 2018).

Competition Issues

An interesting but perturbing facet of e-commerce is the dominance of the sector by the platforms owned by a few multinational companies as these entities are perceived by consumers to be more reliable than the lesser known MSMEs. The data collected by these dominant platforms increases with the number of users that include consumers, traders and service providers. More users lead to greater revenue for the platforms including from advertisements. Large platforms also have the ability to reduce transaction costs for users. However, capturing of markets by a few players usually leads to anti-competitive practices including abuse of dominant position. This includes sale of product or services at a very low cost through discounts to reduce or eliminate competition, denying or limiting market access to others and unfairly pricing product and services. Such a scenario also results in concentration of wealth in the hands of the few dominant players. The issues related to competition are covered under GATS Article VIII (Monopolies and Exclusive Service Suppliers) and IX (Business Practices). Article VIII provisions are aimed at ensuring that the monopoly suppliers from a Member country do not abuse their monopoly position in the territory of another, while Article IX recognises that certain business practices of service

suppliers that are not monopolies could also restrain competition and thereby restrict trade in services (WTOc). Competition issues were taken note of in the discussions at the Work Programme on e-commerce. The Members had opined that though the expansion of the sector could lead to the entry of smaller service suppliers and, in turn, reduction of the extent of restrictive business practices, there were concerns regarding monopolies and restrictive business practices hampering e-commerce. Members, therefore, wanted a closer look into the issue (WTO, 1999).

Digital Divide

The term 'digital divide' came into use in the late 1990s when it was defined as 'the divide between those with access to new technologies and those without' (NTIA, 1999). The OECD then defined it in a broader manner as "the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access Information and Communication Technologies (ICTs) and to their use of the Internet for a wide variety of activities. The digital divide reflects various differences among and within countries" (OECD, 2001). In order to engage and gain from e-commerce and the digital economy, countries will have to ensure that individuals and MSMEs, even in the remote areas, have affordable access to ICTs. They will also have to ensure that individuals are skilled in the latest digital technologies. However, there exists a wide gap between developed and the developing countries in terms of 'the share of population using the Internet, share of population with an account ownership at a financial institution or with a mobile money service provider, availability of secure Internet servers, and postal reliability' (UNCTAD, 2019d).

Reshoring

There is also another cause for worry for the developing world. What was gained by many developing countries earlier through offshoring of activities from rich countries with high labour costs could be lost due to reshoring of these activities to those developed countries that now have advanced manufacturing and service facilities equipped with 3D printing, robotics, Internet of Things, artificial intelligence and Big Data analytics. In this regard, it is important to look at ways to help bridge the digital divide including by helping boost the institutional and regulatory capacity of developing nations and ensuring the effective use of the Aid for Trade initiative. Also, it is crucial to discuss possible measures to transform developing countries and LDCs into exporters of digitised items. In the light of the cross-cutting nature of digital technology issues and efforts for rule-making on e-commerce at the WTO, there are calls for greater coordination of the WTO with other international bodies. However, there are objections too from Members against the push for bringing issues that are discussed in other global bodies into the WTO without first identifying whether such efforts are in line with the agreed WTO norms (WTO, 2018d).

Lessons from Regional Trade Agreements and WTO Discussions

Several Regional Trade Agreements (RTAs) have incorporated various norms relating to e-commerce. These RTAs include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the EU's pacts with Japan, South Korea and Canada, South Korea's agreements with the US, Canada and Australia, the U.S.-Australia agreement, and Australia's pact with China and Japan. The e-commerce provisions range from those meant for basic cooperation to hard commitments; and from general provisions (related to transparency, dialogue and non-discrimination) to trade-facilitation measures such as those including e-signature and e-certification related to paperless trading. They also include norms to ensure consumer and data protection, prevention of spam, cyber security, and further

to address technological issues such as those related to free flow of data across borders and non-disclosure of source code (Ptashkina, 2018).

Another study found that as of September 2017, there were around 69 RTAs with norms relating to e-commerce, starting from the Australia-Singapore Free Trade Agreement (FTA) that came into effect in July 2003. Interestingly, it was found that not only the pacts between developed countries, but also those involving developing countries (for instance, the Costa Rica-Colombia FTA) had e-commerce provisions covering various aspects including those related to consumer protection and paperless trading. The provisions in RTAs also address the issue of defining what constitutes a digital product, electronic authentication, e-transmission and spam. They also had norms on ensuring market access for digital products to the partner countries by agreeing to do away with custom duties on digital products (Wu, 2017). Yet another study, analysing 275 RTAs in force and notified to the WTO as of May 2017, found that 75 of them had at least one provision overtly related to e-commerce. It also found that most prevalent e-commerce norms relate to cooperation, promotion of the sector and on the moratorium on customs duties. Other e-commerce provisions were regarding consumer protection, protection of personal data, electronic authentication, paperless trading and related to domestic legal framework (Monteiro and Teh, 2017).

However, these commonalities in RTAs may not necessarily make it easier to start or forge an e-commerce agreement at the WTO level. This is because the comfort that a country has for including e-commerce provisions in a pact at the bilateral or regional level would not be the same, or would even be entirely missing, when it comes to entering into multilateral negotiations on e-commerce with other Members at the WTO. So, the best alternative would be to go in for plurilateral negotiations with like-minded Members, with an option for other countries to join when they are ready. However, even negotiations on a plurilateral agreement would encounter challenges relating to varying views on the issues involved, given the complexities due to lack of harmonisation of national legal frameworks on e-commerce at this stage (Wu, 2017). The evolution of discussions on the topic at the WTO can be seen in Box 3.1.

Box 3.1: Timeline of Major Developments Related To WTO Discussions

December 1996 - Singapore Ministerial Conference witnessed the conclusion of the Information Technology Agreement (ITA) by 29 Members, aiming to liberalise and eliminate tariffs on IT products covered under the pact. Currently, the pact has 82 Members as signatories, which account for 97 per cent of global trade in IT products (WTOc).

May 1998 - WTO Members, at the Second Ministerial Conference, recognised the growing potential of global e-commerce to generate new opportunities for trade. They adopted the *Declaration on Global Electronic Commerce*. The Declaration stated that the practice of not imposing customs duties (or a moratorium on customs duties) on electronic transmissions will continue. It called for setting up of a comprehensive ***Work Programme on e-commerce*** by the General Council. The aim was that all trade-related global e-commerce issues, including the Member-identified ones, were to be looked into by the Work Programme (WTO, 1998d).

September 1998 - The General Council adopted the Work Programme on e-commerce (WTOe). The Council for Trade in Services was asked to look at the treatment of e-commerce under in the GATS legal framework, while the Council for Trade in Goods was instructed to examine the related aspects of e-commerce relevant to GATT 1994 provisions, etc. The Council for TRIPS was directed to study the intellectual property issues linked to e-commerce, while the Committee on Trade and Development was asked to report on the development implications of e-commerce, taking into account the financial, economic and development needs of developing countries.

Box 3.1 continued...

Box 3.1 continued...

June 2001 - The first dedicated discussion on e-commerce was held under the auspices of the General Council to address cross-cutting issues. These issues included: (i) *'classification'* (definition, technological neutrality, etc. as well as the 'lack of clarity with regard to the classification under GATT/goods or GATS /services of certain products that can be delivered both in electronic form and on a physical carrier'); (ii) ways to ensure that benefits of e-commerce flow to developing countries including by way of technical assistance, capacity building and transfer of technology as well as by narrowing the digital divide and by facilitating easier movement of natural persons; (iii) fiscal implications and imposition of customs duties on e-commerce; competition (concentration of market power, IPRs), jurisdiction and applicable law etc (WTO, 2001).

December 2015 - At the Nairobi Ministerial Conference, more than 50 Members announced that they have concluded the expansion of the Information Technology Agreement. The coverage of the pact included an additional 201 items valued at over $1.3 trillion annually (WTO, 2015).

June and November, 2016 - The Council for TRIPS held its initial discussion of issues concerning IPR protection and enforcement in the context of e-commerce. As per the December 2016 Report on the review of progress of the e-commerce Work Programme, some Members felt that "e-commerce was being given a higher priority as compared to the Doha issues of interest to them" and that "some of the submissions went beyond the exploratory nature of the Work Programme and were looking towards rule-making" (WTO, 2016a).

2016 - WTO reported that since mid-2016, 25 submissions were made to the General Council and to the relevant WTO bodies seeking to collate e-commerce issues relevant to trade policy, calling for setting up a central locus to discuss all e-commerce matters, and demanding rule-making on copyright, e-signatures and consumer protection (WTOa).

July 2016 - MIKTA countries (Mexico, Indonesia, Korea, Turkey and Australia) convened an e-commerce workshop in a bid to ensure more attention on digital trade discussions at the WTO (WTO, 2016b).

2017 - In the run up to the 11th Ministerial Conference (MC11), Members submitted papers with greater focus on the issue; and as part of MC11 preparations, the Chair of the General Council held bilateral consultations and informal open-ended meetings with Members. The focus areas were: (i) the moratorium; (ii) the future of the Work Programme; (iii) possible e-commerce negotiations; and (iv) formation of an institutional mechanism on the lines of a Working Group (WTOa).

February 2017 - Trade Facilitation Agreement entered into force following two-thirds of the WTO membership ratifying it. The pact is expected to result in major automation of border management and simplified norms that boost e-commerce (WTOf).

April and December 2017 - "Friends of E-Commerce for Development" (Argentina, Chile, Colombia, Costa Rica, Kenya, Mexico, Nigeria, Pakistan, Sri Lanka and Uruguay) held their first (in April) and second (in December) Ministerial Meeting to take forward discussions on e-commerce at the WTO. The second meeting was attended by non-member countries including such as Bangladesh, Brazil, Cambodia, Paraguay, Singapore and Thailand. China joined the group in September 2017 (UNCTAD, 2017b and Govt. of China, 2017).

December 2017 - WTO, the World Economic Forum and the Electronic World Trade Platform (eWTP) launched a new initiative called 'Enabling E-commerce' with an objective to boost public-private dialogue on e-commerce by starting a conversation between businesses, governments, and other stakeholders on ways to ensure that small businesses gain from e-commerce policies and practices. (WTO, 2017b). Also, a group of 71 developing and developed countries, accounting for 77 per cent of global trade, jointly proposed to initiate "exploratory work together toward future WTO negotiations on trade-related aspects of e-commerce" (WTO, 2017a).

October 2018 - E-commerce was the focus area at the WTO Public Forum with a high-level panel session including the WTO, the WEF and the eWTP. The session saw a debate on the issue of enabling an inclusive future for e-commerce (WTO, 2018e).

Box 3.1 continued...

Box 3.1 continued...

January 2019 - 76 WTO partners, including the European Union, its member States and 48 other WTO Members, confirmed their intention to start WTO negotiations on trade-related aspects of e-commerce and aim for a 'high standard outcome'. They kept the initiative - which recognises the challenges faced by developing countries, LDCs and MSMEs regarding e-commerce - open to all WTO Members (WTO, 2019c).

April 2019 - The EU submitted its proposal for WTO rules on e-commerce demanding norms on: e-contracts, e-authentication and e-signatures (for paperless trade), consumer protection including redressal measures, protection of personal data and privacy, spam prevention, net neutrality and open internet access to help small businesses to go global, moratorium on customs duties on e-transmissions, not requiring transfer of/access to source code of software and not restricting cross-border data flows through data localisation requirements (WTO, 2019d).

June 2019 - India and South Africa brought out a joint paper at the WTO on: (i) revenue implications of the moratorium on electronic transmissions; (ii) scope and definition of electronic transmissions; (iii) technical feasibility of imposing customs duties on electronic transmissions; and (iv) broader impact of the moratorium on trade and industrialisation (WTO, 2019e).

June 2019 - G20 Finance Ministers and Central Bank Governors endorsed the ambitious work programme on addressing the tax challenges arising from digitalisation. They also agreed to expedite efforts to arrive at a consensus-based solution on the issue by the year 2020 (G20, 2019a).

June 2019 - 23 countries and the EU issued the "Osaka Declaration on Digital Economy" and launched the "Osaka Track". The initiative was aimed at taking forward the efforts towards global rule-making on digital economy, particularly on data flow and e-commerce. The official statement said the move 'will provide a political impetus to the negotiations on e-commerce at the WTO in order to move forward in a fully-fledged manner' (G20, 2019b).

December 2019: Members of the WTO decide to extend the moratorium on customs duties on electronic transmissions till the 12th Ministerial Conference (MC12) slated to be held in June 2020 in Kazakhstan. The members also decided to take forward their work under the extant 1998 work programme on e-commerce in the early part of 2020 and this will include 'structured discussions' to help ministers 'take an informed decision' by MC12. (WTO, 2019f)

Source: WTO, UNCTAD, Govt. of China, G20.

The proposals submitted by various members at the WTO have reflected the divergence of views.

Costa Rica wanted the continuation of the existing Work Programme on e-commerce. However, it sought a WTO E-Commerce for Development Agenda to be integrated into the Work Programme to focus on: *(i) addressing the digital divide from the Sustainable Development Goal 9(c) point of view, which is "to significantly increase access to ICT and strive to provide universal and affordable access to the Internet in LDCs by 2020"; (ii) boosting trade from developing countries, particularly from LDCs, to developed countries through e-commerce by simplifying customs procedures; (iii) facilitating access to finance for LDCs and MSMEs to be active in e-commerce (iv) facilitating mobile payment services to enhance financial inclusion, and to ensure greater e-commerce transactions; (v) improving norms related to data protection, consumer protection and secure cross-border data transfers; and (vi) getting the assistance of global institutions such as the WTO, UNCTAD and International Trade Centre (ITC) for MSMEs in e-commerce skills development and technical assistance.* The communication also sought the submission of a progress report on the WTO's E-Commerce for Development Agenda before the General Council. It wanted the WTO E-Commerce for Development Agenda to identify priority needs of developing countries, including LDCs, landlocked developing

countries, and Small Island Developing States regarding e-commerce (WTO, 2017c).

The African Group, in their statement, disagreed with the idea of taking the discussions beyond the current structure or institutional arrangement of the Work Programme and opposed efforts to set up a Working Group on E-commerce. The African Group said establishing a Working Group to start negotiations would amount to a 'top-down' approach, which it said was unacceptable. According to the African Group, such an approach would go against the prevailing 'bottom-up' structure of the Work Programme, where "the technical issues were dealt with in the technical bodies first, and upon maturity, would be taken to the General Council." The African Group also said it is currently premature to move towards rule-making on e-commerce as "discussions (at the Work Programme), even from a trade policy perspective have not been adequately explored, and where it has, it has barely touched the surface." The Group was also against automatic renewal of the moratorium on customs duties pending discussions on its revenue implication, especially in the context of growing digitisation of goods and services. Besides, the African Group opposed the push for 'free flow of data, no data localisation requirements, permanent moratorium on customs duties, non-disclosure of source code and prevention of forced technology transfer.' Noting that even the current multilateral rules are limiting the policy space of African governments, the African Group stated that rule-making on new issues such as e-commerce would "entrench existing imbalances and further constrain the ability of our governments to implement industrial policy and catch-up" (WTO, 2017d).

China, which also supported the continuation of the Work Programme, however, wanted the General Council to emphasise the development dimension in the Work Programme, and appoint the Chair of the Dedicated Discussion. It also pitched for the Dedicated Discussion to take up 'trade-related e-commerce elements acceptable to Members, including but not limited to facilitating cross-border e-commerce; promoting paperless trading; transparency; as well as development and cooperation' (WTO, 2017e). According to China, e-commerce negotiations at the WTO should be development-oriented, in the sense that it should favorably consider the concerns of developing Members including the LDCs. The negotiations should be transparent, consensus-based and ensure a balance among issues such as 'technological advancement, business development and legitimate public policy objectives of Members, such as internet sovereignty, data security and privacy protection,' China stated. On the issue of customs duties moratorium on e-transmissions, China wanted the continuation of the existing practice of a temporary moratorium, and not a permanent one. It also sought a proper definition of 'trade-related aspects of e-commerce as well as e-transmission,' and clarity on the relationship between future e-commerce rules and the existing WTO Agreements. China also wanted Members to 'respect the internet sovereignty, exchange best practices, enhance e-commerce security, deepen cooperation, and safeguard the cyber security.' On issues such as data flow, data storage and treatment of digital products, China cited the sensitivities and complexities involved as well as the 'vastly divergent views' among the Members and sought greater discussions before taking them up for negotiations. In all, China argued for measures to facilitate e-commerce transactions and establish a trust-worthy environment for the same, as well as for taking steps to bridge the digital divide and promote inclusive development cooperation (WTO, 2019g).

Australia, Canada, Chile, Colombia, the European Union, South Korea, Mexico, Montenegro, Norway, Paraguay, Peru and Ukraine wanted to build upon the Work Programme and establish a Working Party, which would report periodically to the General Council (WTO, 2017f).

At the Buenos Aires Ministerial, **India** pitched for continuation of the Work Programme. However, it also stated that its approval for the temporary extension of moratorium on e-transmissions would be subject to a similar approval by all the Members for temporary extension of the moratorium on Non-Violation (and Situation) Complaints (NVC) under the Trade-Related aspects of Intellectual Property rights agreement (TRIPS) (WTO, 2017g). NVC refers to the situation where a country approaches the WTO Dispute Settlement Body even when a WTO agreement has not been infringed. The apprehension was that developed countries (that house several big pharmaceutical companies with patents on several drugs) could make use of NVC against developing countries (that are among the leaders of generic pharmaceuticals, which includes off-patent drugs) as part of efforts to ensure protection to patents. With its own demand for a 'permanent moratorium' on NVC, India effectively countered the demand from the developed countries for a permanent moratorium on e-transmissions. This strategy of India ensured that there was no decision at the Buenos Aires Ministerial Conference on a permanent moratorium on e-transmissions.

Bangladesh also wanted the retention of the Work Programme, but it demanded that the General Council should examine the development of e-commerce to ensure that the potential of the sector benefits SMEs in developing countries, especially LDCs. It also wanted the Director General of the WTO to work closely with other global bodies on issues relating to bridging the digital divide, ensuring access to internet for all, e-payment solutions, cyber-security and consumer policy. Significantly, it wanted developed countries and the better-off among the developing countries 'to provide duty free and quota free access to all goods and services originating from all LDCs that are exported using e-commerce platform directly from LDCs suppliers' (WTO, 2017h).

A day prior to the December 10-13, 2017 Buenos Aires Ministerial Conference, **Bangladesh, Panama and Singapore**, in a joint communication to the WTO, summed up the options on e-commerce with an aim for it to be considered for a draft ministerial decision on the topic.

According to the communication, there were four ***options*** *on the table* ***regarding the future work on e-commerce at the WTO***.

These included: (i) ***Continuation of Work Programme*** (proposed by India, African Group and Bangladesh); (ii) ***Formalisation of Dedicated Discussion*** (proposed by China, Singapore, Panama, Qatar, and Laos); (iii) ***Working Group with Discussions*** (proposed by Russia, Japan, Costa Rica, Switzerland, Taiwan, Penghu, Kinmen and Matsu, and Hong Kong); and (iv) ***Working Party and mandate to discuss, assess and negotiate*** (proposed by EU, Australia, Canada, Chile, Colombia, the Republic of Korea, Mexico, Montenegro, Norway, Paraguay, Peru, Ukraine, New Zealand and Israel).

Two options were proposed for the manner in which discussions on the list of issues would take place. These included: (i) On the basis of the proposals of Members; and (ii) Members' submission on topics for discussion in the Working Group/Working Party/Dedicated Discussion/relevant bodies. It was proposed that the topics could include (but not limited to): ***(a) priority needs of developing country Members, particularly those of LDCs, with respect to development of infrastructure for e-commerce, technical assistance and capacity building; (b) barriers for access to e-commerce by MSMEs; (c) facilitation of cross-border e-commerce; (d) promotion of paperless trading; (e) transparency, and development and cooperation; (f) definitions; (h) gaps in the WTO legal framework; (i) intellectual property rights; and (j) measures Members have taken and may take to develop their national institutional regulatory capacity that ensure the protection***

of information of all Members and their citizens, including mandatory disclosure of data, the disclosure of source codes, access to, and transfer of technology.

Similarly, on the issue of ***e-commerce moratorium*** also two options on the table were highlighted. These included: (i) ***automatic renewal for another two years*** (i.e, from 2017 until 2019); and (ii) ***non-automatic renewal, subject to other decisions.*** For instance, the African Group wanted discussions on revenue implications of the moratorium on customs duties, especially from the perspective of growing digitisation of goods and services, while India wanted decision on renewal of moratorium linked to decision on moratorium on TRIPS NVCs. And lastly, it was proposed that a Ministerial Decision on e-commerce should also include the Bangladesh's proposal on ***Duty Free and Quota Free (DFQF) access*** to all LDC goods and services exported using e-commerce platform (WTO, 2017i).

Following the Buenos Aires Ministerial Conference, which witnessed 71 proponents jointly calling for initiating exploratory work together toward future WTO negotiations on trade-related aspects of e-commerce, several detailed proposals were submitted by a few developed and developing Members at the WTO in a bid to take forward that agenda.

Argentina, Colombia and Costa Rica said negotiations must focus on clarifying prevailing WTO disciplines and on bringing out new rules where necessary so that new developments or gaps in the system can be addressed. They proposed a broad outline for a negotiating agenda. Their concern was over limiting the focus to just trade as, according to them, e-commerce is multifaceted. Therefore, they wanted a comprehensive agenda and a negotiated outcome covering all relevant WTO disciplines, as well as attention to initiatives that can take care of the interests of developing countries and LDCs. These countries also sought flexibility for developing countries in binding market opening and undertaking new commitments on regulatory matters. They also stated that negotiations should lead to bindings of market opening in e-commerce-related sectors of trade in goods and services. Besides, they wanted the negotiations to address regulatory issues to ensure protection of privacy of individuals as well as security and confidentiality of information (WTO, 2018f).

New Zealand pointed out the existing work done at the WTO and asked Members to rely on such work instead of duplicating the same. It proposed a list of topics that could be considered for discussion. These included: (i) trade facilitation provisions (including a basic domestic electronic transactions framework for electronic contracting in line with international best practice; paperless trading and electronic authentication and recognition of e-signatures); (ii) permanent moratorium on customs duties on e-transmissions; and (iii) consumer focused norms including protection of personal information and spam-prevention measures (WTO, 2018g).

Brazil, in its proposal, wanted the exploratory work to include negotiating pillars of market access (by pursuing work under existing GATT and GATS rules), e-commerce facilitation (consumer protection and spam prevention) and e-commerce development (including issues such as the use of e-payment systems; remuneration of artists and performers). It also sought a *reference paper* on matters such as: *(i) voluntary adoption of international standards of privacy; (ii) jurisdiction and the ability to enforce national law; (iii) disciplines on the usage of big data; (iv) ownership of data produced in different jurisdictions; (v) rules applicable to online platforms and their algorithms; and (vi) issues related to large online platforms including competition law, data portability and non-discriminatory access.* This, Brazil said, should be in addition to developing general principles including on: *(i) free and open internet; (ii) right of the nations to retain their policy space to regulate in the public interest; (iii) greater*

access and participation of women as consumers and as traders in e-commerce; and (iv) addressing the challenges of MSMEs (WTO, 2018h).

In its revised proposal, Brazil brought in 'principles on access to and use of the internet for digital trade' with reference to measures that would ensure that consumers get to access and use services and applications of their choice. The proposal also covered measures on consumer protection, personal data protection, cyber security, paperless trading, spam prevention, e-signature, e-contracts and digital certification in addition to steps to boost regulatory cooperation. It pitched for free cross-border data flows and a moratorium on customs duties on e-transmissions. However, it argued for flexibility for nations to take measures to curb cross-border data flows for achieving legitimate public policy objectives in a manner that they would not be arbitrary or unjustifiable discrimination or a disguised barrier to electronic trade. Also, it proposed allowing countries to impose WTO-compliant internal taxes, fees or other charges on e-transmissions or revenue and profit generated from digital trade (WTO, 2019h).

Japan called for steps to promote harmonisation and interoperability of various domestic regulatory frameworks, ensuring accessibility to various online payment solutions, and allowing cross-border transfer of information by electronic means to facilitate MSME participation in Global Value Chains. It also sought prohibition of data localisation such as using or locating computing facilities, as well as an agreement by Members not to impose untenable curbs on access to any particular websites or services and supply of any particular services both locally and cross-border. Besides, Japan wanted Members to establish clear administrative due process in government access to privacy/industry data. In addition, it demanded that data which are gathered by governments - such as statistical information, data on public transport and data on disaster prevention - should be accessible on a non-discriminatory basis to foreign firms as well to promote innovation. It also wanted Members to improve market access commitments in e-commerce or digital trade related services to 'modernise WTO schedules so as to bring them more in line with commitments achieved in RTAs.' Besides, Japan stated that disclosure of trade secrets including source codes and proprietary algorithms as well as mandatory introduction of particular technologies including encryption technology by a government should be prohibited. It also wanted Members to make information on their respective regulations related to e-commerce or digital trade available to all, through the WTO website (WTO, 2018i).

The U.S. cited the huge growth in cross-border data flows and its importance to international trade, and pitched for transfer of data across borders without arbitrary or discriminatory restrictions. It sought steps to prevent data localisation and web blocking. Its other demands included duty-free and non-discriminatory treatment of digital products, protection of source code, and prevention of forced technology transfer. The U.S. also sought the prohibition of the requirement to use a national technology as a condition of market access. Besides, it argued against restricting the use of encryption and mandating country-specific encryption standards. It also sought greater market access through its demand for new commitments by Members under the GATS that permit the cross-border supply of internet-enabled services, which compete against traditional communication services. The U.S. also wanted countries to agree that old classifications and commitments under GATS can apply to new technologies. It said the services classifications - on which specific commitments are made under the GATS - are outdated, especially for communications services. Like Japan, the U.S. also advocated open government data (WTO, 2018j).

Reiterating most of the above-stated demands, the US had in April 2019 tabled another paper that also sought greater freedom of operations for interactive computer service ('a system or service providing or enabling electronic access by multiple users to a computer server'). Besides it also called for inclusion of 'market access' and 'national treatment' in the proposed WTO digital trade pact (WTO, 2019i). It was observed that the proposal was more or less similar to the digital trade chapter of the U.S.-Mexico-Canada Agreement (which is awaiting ratification) (Baschuk, 2019).

The European Union (EU) proposal argues against imposition of customs duties on e-transmissions, the requirement of access to the source code and data localisation. However, it sought high standards for the protection of personal data and privacy – by applying norms on cross-border transfer of personal data - to enable trust in the digital economy and to the development of trade. Besides proposing a major revision of the WTO reference paper on telecommunications services, it wanted Members to make commitments on computer services and telecommunications services, as well as join the Information Technology Agreement and its expansion (WTO, 2019d).

Singapore, in addition to the suggestions on possible elements for exploratory work on e-commerce and development (Table 3.2), also submitted a text clearly bringing out the issues identified in the exploratory discussions that fell under three broad categories namely: *(i) 'enabling end-to-end cross-border e-commerce'; (ii) 'openness and e-commerce'; and (iii) 'trust and e-commerce'*. These were then divided into various sub-heads and the related proposals. Under 'enabling e-commerce' the sub-heads and proposals included *(i) 'paperless trading' (the proposal was for an agreement to maintain and accept e-versions of documents as well as cooperate to boost such practices); (ii) 'moratorium on customs duties on e-transmissions' (for an agreement to ban customs duties, and also to impose WTO-compatible internal taxes or other charges); (iii) 'domestic e-transactions framework' (for an agreement to maintain such a framework but avoiding any unnecessary regulatory burden on e-transactions); (iv) 'e-authentication and e-signatures' (for an agreement to encourage the use of interoperable electronic authentication and not denying the legal validity of a signature solely on the basis that it is in electronic form); (v) 'e-invoicing' and (vi) 'electronic transferrable records' [under both the above (v) and (vi), for an agreement to encourage them as well as to ensure mutual recognition and interoperability].* Under 'openness and e-commerce', the sub-heads included cross-border data flows (including personal information) and location of computing facilities. The proposals under these were to allow free cross-border data flows and ensure that there is no pre-condition of data localisation. However, it was recognised that there should be room for restrictive measures to achieve legitimate public policy objectives provided that such steps would not be 'arbitrary or unjustifiable discrimination or a disguised restriction on trade'. Under 'trust and e-commerce', the issues included *(i) 'principles on access to and use of the internet for e-commerce' (to enable consumers to access and use services and devices of their choice and to access information on the network management practices of their internet access service supplier); (ii) 'source code' (for an agreement to not require disclosure of source code except that of the software used for critical infrastructure; the proposal also pitches for safeguards against unauthorised disclosure); (iii) measures to prevent spam; (iv) ensuring personal information protection; and (v) online consumer protection* (WTO, 2019g).

Table 3.2: Singapore's suggestions on possible elements for exploratory work on e-commerce and development

Trade Facilitation:		
Issue	*Possible Option(s) for Consideration in Exploratory Work*	*Why?*
Paperless Trading	•Promoting paperless trading in trade facilitation. E.g. Improving existing norms on acceptance of electronic trade administration documents and single window. •Making available electronic versions of trade administration documents to the public.	•Lowers cost of trading and transaction time by simplifying trade facilitation procedures. •Lower cost and simplified procedures lower barriers to entry for MSMEs. •Increases the ease of doing business online.
Moratorium on Customs Duties on Electronic Transmissions	•Making the moratorium permanent.	•Provides certainty for businesses that countries will not impose additional layers of custom duties in the future.
Infrastructure Gaps:		
Issue	*Possible Option(s) for Consideration in Exploratory Work*	*Why?*
Services Market Access and Regulatory Issues	•Identifying specific commitments in services sectors that could enable and promote infrastructure development. •Identifying regulatory issues that could enable and promote infrastructure development (e.g. WTO Telecommunication Reference Paper).	•Encourages investments in services sectors that could enable and promote infrastructure development (e.g. telecommunication services). •Promotes development of services sectors that enable infrastructure development for e-commerce.
Access to Payment Solutions and Online Trust:		
Issue	*Possible Option(s) for Consideration in Exploratory Work*	*Why?*
Electronic Authentication and Digital Certificates	•Ensuring domestic law in place to recognise electronic authentication methods, e.g. electronic signatures. •Mutual recognition or interoperability of electronic authentication and digital certificates.	•Provides certainty for businesses and enhances business efficiency. •Promotes adoption of online transaction methods, and electronic payment solutions.

Table 3.2 continued...

Table 3.2 continued...

Consumer Protection	•Adopting of measures/laws to protect online consumers from fraudulent and deceptive commercial activities. •Promoting of international cooperation between consumer protection agencies.	•Creates a more secure environment for e-commerce activities. •Improves trust, and promotes use of online payment solutions for businesses, and consumers. •Cooperation promotes sharing of best practices among consumer protection agencies, and increases transparency on parties' domestic regulations.
Unsolicited Electronic Messages (Spam)	•Adopting and maintaining measures to protect consumers from unsolicited electronic messages.	•Creates a more secure environment for e-commerce activities. •Builds consumer trust and encourages use of e-commerce.
Protection of Personal Information	•Adopting and maintaining measures or legal framework that provides for the protection of personal information.	•Creates a more secure environment for e-commerce activities. •Improves trust, and promotes use of online payment solutions for businesses, and consumers.
Cooperation in Cyber security	•Recognising the importance of building cyber security capabilities. •Promoting collaboration especially in the areas of identifying cyber security threats.	•As online transactions become more prevalent, cyber security will become a growing concern amongst businesses. Establishing a common understanding of its importance could promote a safer online environment.
Issue	*Possible Option(s) for Consideration in Exploratory Work*	*Why?*
E-commerce and Development: *Trade Facilitation and E-commerce*: Cross-border e-commerce involves low value shipments and/or digital transmissions over the internet. Once within the borders, logistics players also play a big part in ensuring smooth delivery of products. What can be done to further empower smaller business using e-commerce and lower their cost of conducting trade? *Infrastructure Gaps to Enable E-commerce*: Infrastructure gaps in developing countries have posed challenges (e.g. access to broadband) but also provided innovative opportunities for businesses (e.g. rise of local payment solutions). Is there a way to better target technical assistance towards plugging the critical gaps? *Access to Payment Solutions*: Being able to find payment solutions is the key to whether a business will go online. In the absence of secure online payment services, payment via mobile phones and cash on delivery option has been used. How can we improve businesses' and consumers' access to more payment options to better enable them to conduct and access cross-border e-commerce? *Online Security*: Trust is crucial in determining whether consumers are willing to engage in e-commerce. This includes trust in online payment services; reputation of the online merchant and even in whether there is enough legal protection to provide recourse should a transaction goes awry. What can be done to build trust in online transactions and e-commerce and improve consumer protection? Is there scope for improved cooperation between countries on cyber-crime?		

Source: (WTO, 2018k).

India and South Africa, in their joint paper addressed the issues of the revenue implications of the moratorium, definition of e-transmissions, technical feasibility of imposing customs duties on e-transmissions and the broader impact of the moratorium on trade and industrialisation. On the issue of revenue implications, they cited a recent UNCTAD study that had estimated the potential tariff revenue loss to developing countries at USD 10 billion, to WTO LDCs at USD 1.5 billion, to Sub-Saharan African countries at around USD 2.6 billion, as against USD 289 million to WTO High-Income Members. It was shown that by imposing customs duties on e-transmissions, developing country Members (with high bound duties on physical imports of digitisable products) can generate 40 times more tariff revenue as compared to the developed countries (with almost nil bound duties on physical imports of digitisable products). India and South Africa countered the claim of some Members that levying other taxes and internal charges (GST and VAT) could act as an offset against the tariff revenue loss on account of the moratorium. They cited OECD reports to show the challenges of taxing digital businesses as such corporate entities resort to tax avoidance strategies that take advantage of the loopholes in the laws by artificially shifting profits to low or no-tax havens. The joint paper also brought out the differences between Members on the critical issue of whether or not 'content' is covered under the definition of 'e-transmissions'. While some countries had claimed that the moratorium covers 'contents' transmitted electronically, others such as Indonesia stated that in their understanding, the extension of the moratorium would be applicable only to the e-transmissions and not to products or contents submitted electronically. Referring to such differences and its implications for calculating revenue losses, India and South Africa wanted the Members to come to a consensus on the issue before the review of the moratorium in December 2019. Citing the example of Indonesia amending its law in 2018 to impose customs duties on e-transmissions (software and other digital products), the joint paper said that imposing customs duties on e-transmissions may be technically feasible. India and South Africa said according to them 'the customs duty moratorium exists precisely because it is feasible to impose customs duties on such transmissions'. The paper also said it is important for countries to safeguard policy and regulatory space in the WTO to firm up their national digital industrial policies which match the level and pace of their digital development so that they can then build digital capacities to face the challenges of digital trade (WTO, 2019e).

Stances and Objectives

In general terms, the technologically advanced Member countries, mainly the Western countries, have adopted an aggressive approach in e-commerce discussions at the WTO and are keen on negotiations at the multilateral or plurilateral level within the WTO. These countries aim to ensure that the companies headquartered in their territories are able to expand their global footprint by taking over markets especially in the developing world. The other extreme has countries that are small in size and/or population and with hardly any technological prowess or human capacity or financial resources to build their own e-commerce ecosystem. They are, therefore, not against depending on companies with advanced technology in e-commerce that are based mostly in rich countries, for technology-based retail systems as well as for digitised goods and services. These countries also have no overt objections to the launch of e-commerce negotiations at the WTO. Then there are nations like India that not only have a sizeable market but also infant companies with the potential to make it big. Such countries clearly see an opportunity in leveraging their strengths to help their companies scale up globally and improve their economies as well. These countries mostly want greater engagement between WTO Member countries on e-commerce

issues under the existing WTO structure of the e-commerce Work Programme, and have reservations regarding setting up a Working Group to begin formal negotiations. There are also countries like China with a sufficiently large domestic market and companies armed with the latest technology. They are keen on e-commerce facilitation measures to help their own companies grow, but have reservations in opening up their local markets to foreign companies.

As per a recent review of progress of the e-commerce Work Programme, India and South Africa were of the view that the 'impact of the moratorium needed to be understood from the revenue point of view and its continuation should be examined based on concrete facts and statistics'. Other countries were open to having greater research on the scope of the moratorium and pitched for the developmental dimension to be taken into account. There was also the view that moratorium encouraged e-commerce and brought predictability. Some delegations pointed out the difficulties in determining the specific amounts and value of electronic transmissions when it comes to the technical feasibility of imposing customs duties on electronic transmissions. Members were keen to "reinvigorate" the Work Programme and wanted more information to carry out deeper analysis. The chair of the General Council opined that discussions need to continue in a transparent, inclusive and Member-driven manner, keeping in mind the need for a decision on the moratorium by the end of 2019 (WTO, 2018l).

An analysis by Junichi Sugawara (Mizuho Research Institute) of the Japanese initiative

Table 3.3: Stance of Countries on Various Important Issues

Issues	Views
Structure of final agreement	Canada: similar to the Government Procurement Agreement (a plurilateral pact). EU: like the General Agreement on Trade in Services reference paper (so that it remains open to non-signatory members even as it is applicable to the signatories). Saudi Arabia: as an Annex 1 agreement (including the multilateral pact on goods trade, GATS and TRIPS) under the Marrakesh Agreement establishing the WTO. U.S: as a separate Annex 4 agreement (plurilateral agreements applicable only to the signatory members) similar to that in the Marrakesh Agreement.
Definition of e-transmissions	Canada: "digital product" should a computer program, image, sound recording, text, video or other digitally encoded items, that can be electronically transmitted and made for commercial sale or distribution (this is similar to the definition in Canada's trade pacts). Brazil, Japan, South Korea and the US: e-transmission or "transmitted electronically"would mean a transmission made using electromagnetic means (including by photonic/optical etc.) Indonesia: maintain the prevailing practice of moratorium on customs duties on e-transmissions, not including electronically transmitted content. However, this should not prevent a Member from imposing customs procedures for the purposes of public policy or from imposing internal fees, taxes or other charges on e-transmission, provided that such fess, taxes or charges are imposed in a WTO-consistent manner. EU: e-transmissions are only about services; imposing duties on e-transmissions in the future cannot be precluded. U.S: 'Customs duty' includes a duty or any kind of charge imposed on or in connection with import of a good and surtax/surcharge imposed in connection with such importation. However, it doesn't include: (i) antidumping or countervailing duty; (ii) charge equivalent to an internal tax (consistent with Article III:2 of GATT 1994); (iii) fee/other charges linked to the import, and commensurate with the cost of services rendered.

Table 3.3 continued...

Table 3.3 continued...

Permanent moratorium	Cambodia, Indonesia and Malaysia: against permanent moratorium. U.S. and many others: favored permanent moratorium.
Source code	Canada, Singapore, South Korea and the U.S. and some other members of the CPTPP: against any requirement of "transfer of, or access to, source code of software owned by a person of another (Party/Member), (or to an algorithm expressed in that source code,) as a condition for the import, distribution, sale, or use of that software, or of products containing that software, in its territory." China, Saudi Arabia and Russia: were for seeking access to source code due to security concerns.

Source: Washington Trade Daily, 2019. (Author's representation based on the 2 December, 2019 report of the Washington Trade Daily on the fourth round of the Joint Statement Initiative Group on e-commerce at the WTO that concluded on 22 November, 2019).

at the G20 on framing global digital rules in the context of WTO e-commerce discussions showed that the important elements in the proposals at the WTO on the topic were 'facilitation,' 'liberalisation,' 'reliability (trust),' and 'transparency/cooperation/development'. Sugawara then looked at the treatment of these elements in the proposals by Japan, US, EU and China as well as in the recent trade agreements Trans-Pacific Partnership (TPP), United States-Mexico-Canada Agreement (USMCA), ASEAN Agreement on Electronic Commerce and the Japan-EU FTA. It was found that the U.S. and Japan were keen on 'liberalisation' along with 'reliability' and 'facilitation' elements on the lines of TPP and USMCA. Meanwhile, China laid stress on 'facilitation' and 'development' elements, and was not interested in the 'liberalisation' aspects (such as data localisation, market access, free cross-border data flows, open internet, permanent moratorium on customs duties on e-transmissions and non-discriminatory treatment). (See Table 3.4) (Sugawara, 2019).

Table 3.4: Treatment of important elements in recent FTAs and in the proposals by the leading countries/blocs participating in the joint initiative on e-commerce at the WTO

	Elements	FTAs				Proposals			
		TPP	USMCA	Japan-EU	ASEAN*1	Japan	US	EU	China
Facilitation	Electronic signatures and authentications	○	○	○	○	○		○	○
	Paperless trading	○	○		○	○			○
	Electronic payment				○	○			○
Liberalization	Non-imposition of customs duties	○	○	○		○	○	○	△*4
	Free access to the Internet	○	○			○	○	○	
	Non-discriminatory treatment	○	○			○	○		
	Free cross-border transfer of information	○	○		△*3	○	○		
	Data localization	○	○		○	○	○	○	
	Market access	−*2	−*2	−*2		○	○	○	
Reliability (Trust)	Online consumer protection	○	○	○	○	○		○	○
	Unsolicited commercial e-mail	○	○	○		○		○	○
	Protection of personal information	○	○	○	○			○	○
	Source codes	○	○	○		○	○	○	
Transparency/ Cooperation/ Development	Publication and exchange of information on regulations	○	○	○	○	○			○
	Technical assistance and capacity building								○

Notes: *1 ASEAN Agreement on Electronic Commerce
*2 As a comprehensive FTA, provisions on market access are provided in other chapters.
*3 This provision is not obligatory.
*4 This provision does not make the obligation permanent.

TPP – Trans-Pacific Partnership; USMCA - United States-Mexico-Canada Agreement

Source: Sugawara, 2019.

Private Sector Views

Meanwhile, there had been lobbying by business groups for liberalisation of norms to boost global e-commerce. The International Chamber of Commerce (ICC) had demanded that the WTO Member countries must agree to make the moratorium permanent by citing the difficulties in calculating tariffs for e-transmissions as well as in the costs and complexities involved in enforcing customs duties on e-transmissions. It also referred to studies[2] showing that potential tariff revenues from imposition of duties on e-transmissions would be much less than the extent of overall economic losses on account of such a move.[3] Acknowledging the concerns of developing and least developed countries over revenue loss in this regard, the ICC favoured a non-discriminatory, simple and consistent VAT/GST regime instead of customs duties. It also suggested adoption of international best practices in this regard through a consensus-based mechanism at the global level. (ICC, 2019b).

There are views in the private sector as well against stringent norms to regulate e-commerce. The founder of e-commerce major Alibaba, Jack Ma, had gone to the extent of stating that it was too early to regulate the sector since its development was a nascent stage. Another view was that since non-cross border e-commerce and non-cross border online shoppers accounted for the majority of the global e-commerce market and global online shoppers respectively, what was important at this stage was regulating the sector at the domestic level and not internationally. Also, considering the fact that the U.S., China, U.K., Japan, Germany and France dominate the e-commerce market, it was felt that a global e-commerce pact at this stage would be more beneficial to them than to the other economies (Arun, 2017). This is because of the apprehension that any attempt to harmonise e-commerce rules globally could result in a situation of 'Americanization' of e-commerce rules where the standards of the U.S, which is a digital economy giant, would be replicated in other countries through global e-commerce rules. This is what happened in the case of earlier treaty initiatives including the Internet treaties of World Intellectual Property Organization and the Anti-Counterfeiting Trade Agreement where the entrenched business entities use their influence to ensure that rules are made in their favour. Therefore, it is important to first ensure the development of new businesses and new business models. Setting global e-commerce rules including on important aspects such as data transfer, data localisation, disclosure of source code, discriminatory business practices, privacy and protection of personal data even before developing a strong ecosystem that has several new players and new business models will only result in a scenario where the global norms would favour well-established firms and act as entry barriers to the rest. Also of concern would be the secrecy of the rule-making process and inadequate inputs from all the stakeholders. (Geist, 2018).

Society 5.0

Taking a holistic approach, Japan had come up with a roadmap for the future through its plan to realise the concept of 'Society 5.0', which envisions a 'super-smart society' that addresses social challenges by using the innovations of technologies such as big data analytics, Internet of Things, robotics, artificial intelligence and the sharing economy into not just industries but also in all aspects of social life. Collection of data such as personal data including those related to health, medical and financial records as well as commercial data including those from various sectors and data from various modes of transportation forms the basis of this plan. The data is then processed using the latest technologies such as Big Data analytics and used for bringing out various advanced products and services (Govt. of Japan, 2019). Japan, which has the G20 Presidency for 2019, has been pushing the 'digital economy' agenda in the G20. As per the June 2019 G20 Ministerial

Statement on Trade and Digital Economy, the G20 Members looked into various aspects related to the interface between trade and the digital economy including designing and implementing digital policies as well as the concept of a human-centered future society promoted as Society 5.0 in Japan.

Data Free Flow with Trust

Among the matters discussed during the meeting was the initiative of Data Free Flow with Trust (DFFT), which recognises the opportunities as well as the challenges arising from free flow of data. The opportunities include greater innovation, higher productivity and improved sustainable development, while the challenges are related to privacy, security, data protection, intellectual property rights. Significantly, the Ministers agreed that ensuring respect for domestic and international legal frameworks would help build trust and facilitate the free flow of data. They have decided to 'cooperate to encourage the interoperability of different frameworks, and affirm the role of data for development'. The G20 Members also reaffirmed the importance of the WTO Work Programme on e-commerce, but also took note of the ongoing discussion under the Joint Statement Initiative on e-commerce. They have recognised the need to boost investment in ICT infrastructure particularly in developing countries as well as build capacity for MSMEs, women and youth to ensure that they derive greater benefits from participating in the digital economy (G20, 2019c).

The think-tank Information Technology and Innovation Foundation (ITIF) had proposed four core principles and policies to take forward the DFFT initiative. These include: *(i) placing 'accountability' at the centre of the DFFT framework and 'holding firms accountable for managing the data they collect, regardless of where they store, process, or transfer the data'; (ii) ensuring that countries 'put in place new or updated mechanisms to manage cross-border access to data for law enforcement purposes'; (iii) ensuring that countries 'responsibly stop data flows of illegal content'; and (iv) ensuring that countries support (and not undermine) encryption's role in securing data flows'*. The objective is to build trust between countries through these four proposed principles that the ITIF wants countries to consider during their discussions related to e-commerce and data at forums like the WTO (Cory *et al.*, 2019).

G20 and Osaka Track

The G20 platform was further used to give a 'political impetus' to the joint initiative on e-commerce at the WTO that now has the support of 78 WTO members (representing developing and developed countries and regions including Asia Pacific, Africa, Americas, Europe, Middle East and Russia/CIS), up from 71 in December 2017 when the proposal for future negotiations on e-commerce at the WTO was first put forward. On the sidelines of the June 2019 G20 Osaka Summit, a special initiative called 'Osaka Track' was launched to boost the efforts for global rule-making on digital economy. According to Japan, it is important to expedite the framing of global rules and disciplines particularly on e-commerce and its trade-related aspects as well as on data flow to harness the digital economy's full potential to in turn promote innovation (G20, 2019b). Notable G20 member countries that did not sign on to the Osaka Track included India (Govt. of India, 2019a), Indonesia and South Africa. However, these three countries can take heart from China's position that more 'exploratory discussions are needed' on the 'implications and impacts, as well as related challenges and opportunities' of issues such as data flow, data storage and treatment of digital products before taking them up for WTO negotiations. China has also said that though 'trade-related aspects of data flow are of great importance to trade development, more importantly, the data flow should be subject to the precondition of security, which concerns each and every Member's core interests' (WTO, 2019f). However, while China's stand on cross-border flow of data is close to the

position taken by India, Indonesia and South Africa, the trio has adopted a tougher approach by declining to join the Osaka Track and the Declaration despite Japan's assurance that the global framework that it wants to help firm up would be based on the initiative of Data Free Flow with Trust (DFFT) that recognises not only the opportunities but also the challenges are related to privacy, security and data protection (Palit, 2019).

Way Forward

The benefits of the exponential growth in electronic transmissions are now confined to just a handful of economies, mainly in the developed world, that are at the forefront of digital technologies (UNCTAD, 2019a). Incidentally, some of the leading beneficiary economies are the among the WTO members that are the proponents of the joint initiative on e-commerce at the WTO (WTO, 2019c). There are demands from a few of these developed countries to make permanent the temporary moratorium on customs duties on electronic transmissions (WTO, 2018g).

India and a few other developing economies have taken the stand at the WTO that it is important to have greater discussions on the fiscal implications of this customs moratorium on realising the importance of data as the 'new oil' and apprehending the possibility of digital colonisation of the 'data-rich but technologically challenged' economies by the digital multinational companies mostly based in the developed economies. In this regard, the developing countries including India have cited the increase in digitisation of physical products, which is simultaneously leading to a fall in physical trade of those products.

Significantly, this digitisation trend, in turn, is resulting in a loss of tariff revenue, mainly for developing countries that rely on such customs revenues to address their developmental challenges. This issue is especially important due to the discussions at the G20, OECD and various other international platforms and forums on taxing digital companies. India, along with some like-minded countries like South Africa, has also asked the WTO General Council to urgently revisit issues including 'revenue implications of the moratorium on electronic transmissions; scope and definition of electronic transmissions; technical feasibility of imposing customs duties on electronic transmissions; and broader impact of the moratorium on trade and industrialisation.' Their effort is to ensure that discussions at the WTO are confined at this stage to the Work Programme. They want greater attention to be given to possible ways to address the developmental concerns, considering the lack of basic digital infrastructure - including access to secure internet servers as well as to fixed broadband, and an account at a financial institution or with a mobile-money-service provider for making payments - in developing and low-income countries for enabling e-commerce transactions.

Making the temporary moratorium permanent in an urgent manner is not the ideal solution especially when there is a need for greater clarity on the coverage and definitional aspects of the moratorium (that is whether e-transmissions covered under the moratorium refers to electronic carrier medium – be it CDs or electronic bits etc. - or the electronically transmitted content). It was seen the moratorium has resulted in discrimination against local firms and could harm the startup digital companies (Cheng and Brandi, 2019). Besides, there is also a need for countries to gain greater insights into the linkages that e-commerce has with intellectual property (including source code and algorithm besides copyrights, trademarks, patents and trade secrets) for emerging technologies (technologies related to Internet of Things, machine learning, robotics, artificial intelligence and big data analytics). In the meantime, developing countries should consider bringing out mutually helpful policies

on e-commerce and intellectual property to help address their developmental challenges. Such policies should be able find the right balance between intellectual property rights protection and access so that developing countries can take advantage of the opportunities arising out of the e-commerce growth even as they try to protect their policy space for boosting local e-commerce entities in a sustainable manner (Ido, 2019).

Loss of Policy Space

Entering into formal negotiations on e-commerce at this stage - where the main demands include permanent moratorium on customs duties on e-transmissions, non-disclosure of source code, free flow of data across borders without any localisation requirements and prohibition on forced transfer of technology - would mean a loss of policy space for many of these low and middle income countries that are huge sources of data, but are yet to firm up a national policy on e-commerce covering issues including data protection, source code and technology transfer. Also, the local industry in these developing and poor economies would find it difficult to quickly adapt to the proposed rules, if the norms are in favour of big digital companies. Another concern for developing countries is the push for inclusion of new issues such as e-commerce even without the conclusion of several outstanding issues of the Doha Round including those related to food security.

However, this does not mean India and other developing economies should completely disengage themselves from the e-commerce related discussions and developments at the WTO, especially when 76 of the 164 WTO members - accounting for close to half of the WTO membership and around 80 per cent of the world trade - have decided to launch negotiations on global rules on e-commerce (WTO, 2019c).

On the multilateral front, India, Indonesia and South Africa should note that big emerging economies (Argentina, Brazil and Turkey), lower middle income countries from Africa (Nigeria and Senegal) and Asia (Vietnam) as well as LDCs (like the ones such as Laos and Myanmar in Asia) are engaging themselves in the initiative to take forward discussions for global e-commerce rule-making even though they have their own concerns on issues such as security and data protection. Staying out of initiatives such as the Osaka Track, which is based on 'Data Free Flow with Trust' principles, as well as the joint initiative at the WTO - where it has been assured that the 'challenges faced by developing countries and LDCs, as well as by MSMEs in relation to e-commerce' will be taken into account - would prevent India and other like-minded nations from steering the course of these discussions and building a global digital trade framework to their advantage (Palit, 2019). Given the growing importance of e-commerce in world trade, India and other developing countries should study the example of China that has gone on to become a global leader in e-commerce as well as a proponent of the joint initiative on e-commerce rule-making at the WTO even while protecting its national interests through norms including restrictions on cross-border data flows. Simultaneously, the developing countries should ensure that they are not isolated by the e-commerce proponents. To avoid such isolation, the developing countries should build capacity to prepare themselves to engage in technical discussions and negotiations at a later stage at the WTO when there is consensus. They should also form new coalitions to protect their common interests.

India and the other developing countries that plan to stay out of the joint initiative on e-commerce should take into account the fast growth in digital trade, the shortcomings in the current WTO agreements regarding the lack of a proper definition of a digitally traded product and the problems related to the treatment of new digital services under the existing GATS schedules. They should also note the deadlock in multilateral negotiations at the

WTO regarding market access for products and services, the rising importance of data in global trade and the inadequacies of the prevailing WTO regime in addressing issues such as cross-border data flows, consumer protection, cyber-security and facilitation of digital trade.

Owing to these limitations in the existing WTO norms and the tendency of WTO negotiations to be protracted, several countries - including from the developing world and even some of the lower income nations - are opting for bilateral FTAs with specific chapters addressing all the above-mentioned issues regarding digital trade. In its Comprehensive Economic Cooperation Agreement with Singapore, India itself had no problems with a limited number of e-commerce norms (Wu, 2017). It would be important for developing countries like India with a growing digital economy and exports to experiment with more e-commerce provisions in its bilateral agreements to facilitate such digital trade and protect their interests.

As far as the crucial issues of data localisation and cross-border flow of data are concerned, explicit mandatory data localisation measures and prohibition of cross-border data transfer would hurt businesses and consumers alike. Such restrictions would increase the costs related to data storage as well as prevent innovation and startup culture. These curbs would also make it difficult for consumers to choose from a wider and possibly more affordable range of products and services available worldwide.

Balanced Approach

Therefore, countries could consider a balanced approach by incorporating specific conditions in the trade agreements at the multilateral, regional and bilateral levels as well as in the concerned national policies. These conditions could be similar to the EU-U.S. Privacy Shield Framework, where the U.S. would ensure privacy protection of EU citizens to EU standards (including norms on what would constitute adequate level of data protection) in return for personal data transfer from the EU to the U.S. to companies certified in the U.S. as per the Framework norms. However, to implement such a framework, the concerned nations would need to develop their own policies on the lines of the EU General Data Protection Regulation and strengthen enforcement through capacity building initiatives. It would also be important for nations inking such a framework to mutually agree on data sharing arrangement to help their regulators and enforcement authorities to ensure proper implementation of data protection and national security provisions. Data localisation measures could be made partial by specifying its applicability sector-wise and through conditions such as requiring individual consent for cross-border transfer of sensitive data.

Endnotes

1. The four criteria used included: "volume (absolute amount of broadband consumed by a country, as a proxy for the raw data generated); usage (number of users active on the internet, as a proxy for the breadth of usage behaviors, needs and contexts); accessibility (institutional openness to data flows as a way to assess whether the data generated in a country permits wider usability and accessibility by multiple AI researchers, innovators, and applications); and complexity (volume of broadband consumption per capita, as a proxy for the sophistication and complexity of digital activity)"
2. ECIPE, 2019.
3. However, the ECIPE, 2019 study soon attracted criticism (Banga, 2019) on account of reasons including 'flawed definition' of e-transmissions, 'contradictions', 'unrealistic and flawed assumptions', and consequently 'erroneous results'.

IV

India's Draft National E-Commerce Policy

Overview

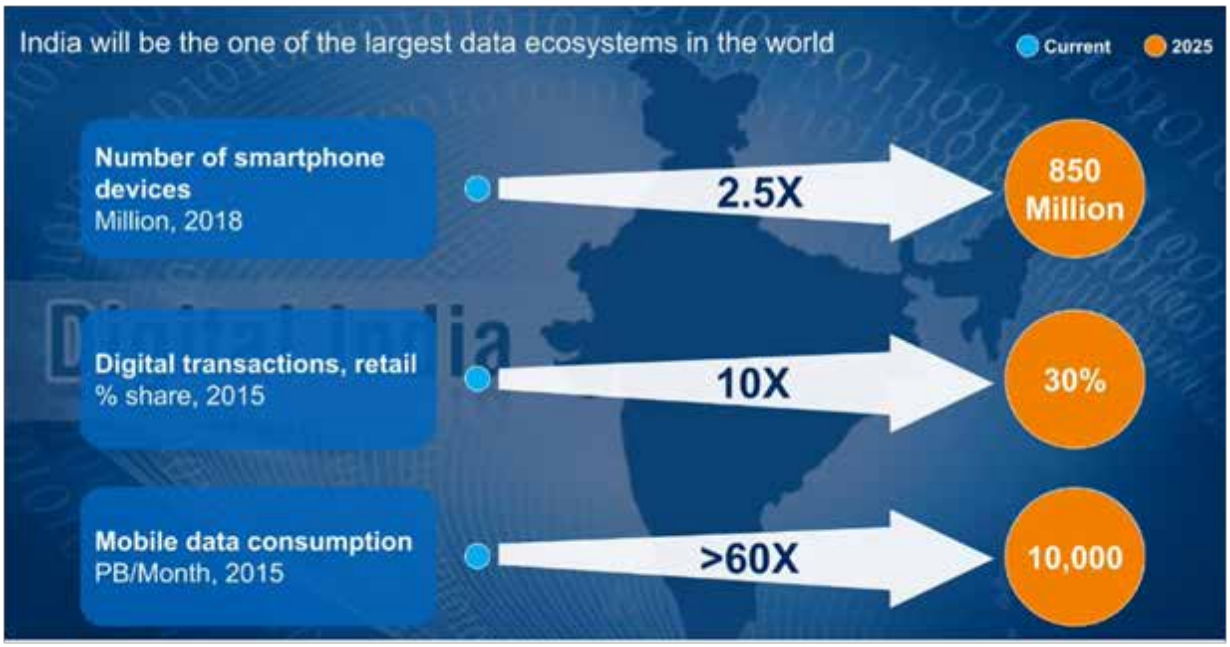
The annual economic value generated by the entire digital economy in India - which includes e-commerce as well as information technology and business process management (IT-BPM), digital payments, domestic electronics manufacturing, digital communication services (including telecom) and direct subsidy transfers – was about USD 200 billion (or 8 per cent of India's GVA in 2017–18). It is estimated that by 2025, this figure could touch USD 800 billion–USD 1 trillion (or value equivalent to 18 to 23 percent of India's nominal GDP). This kind of potential increase in economic value would boost investments in advanced technologies including blockchain, artificial intelligence, robotics and drones that would be customised to the country's requirements. In 2025, the digital economy is expected to support around 60-65 million workers. However, skill development would be crucial for employment growth as sectors such as financial services, transportation, education, tourism, agriculture, construction, manufacturing, logistics and healthcare would become highly digitally-enabled (Govt. of India, 2019b).

India is also expected to have one of the largest data ecosystems in the world by 2025 due to the projected exponential growth in the number of smart phone devices, mobile data consumption and retail electronic transactions (See Figure 4.1).

India is among the fastest growing e-commerce markets in the world. However, it faces several challenges including low internet and smart phone penetration as well as minuscule credit card usage, besides a large unbanked population. The share of e-commerce in the country's total retail is also low (Global Payments, 2018).

E-commerce sector in the country has huge potential, with the market estimated to touch USD 200 billion by 2026 from USD 38.5 billion as of 2017, thanks to the increasing penetration of smart phone and internet. In a bid to take forward the digital economy, the government has taken several initiatives including BharatNet Project (for providing broadband services to villages), Bharat Interface for Money (BHIM, to enable digital payments through a simple mobile based platform), Digital India (to transform the country into a digitally empowered society and knowledge economy) and Startup India (to boost startups). In order to attract greater foreign investments, the government has permitted 100 per cent FDI in B2B e-commerce and 100 per cent FDI through the automatic route in e-commerce

Figure 4.1: The Potential of India's Data Ecosystem



Source: *Govt. of India, 2019c.*

marketplace model. E-commerce retailing in India is witnessing over a million transactions daily with items such as electronics, apparels, home and furnishing, personal care, beauty and baby care items and books being the major ones bought online (IBEF, 2019).

What is also helping the sector is the government's initiative to establish a Government e-Marketplace (GeM), to ensure that procurement of common use goods and services are carried out through the online mode by government agencies.

The e-commerce sector in India presently employs over 100,000 people, mainly in logistics and goods delivery. By 2025, the sector could generate around 500,000 direct jobs. The country has around 176.8 million e-commerce users (in 2017), a huge jump from around 40 million in 2013. Interestingly, despite not having retail infrastructure like that in large metros, consumers in smaller Tier 2 and Tier 3 cities account for over half of the new e-commerce purchases in the country. However, in terms of the usage of digital payments and e-commerce penetration, India is placed lower many peer nations (Govt. of India, 2019b).

E-commerce is also helping the Indian MSME sector in various ways. The MSMEs that are users of e-commerce have seen their marketing and distribution costs falling by over 60 per cent, and have registered 27 per cent higher revenue growth than the MSME firms that are offline. In addition to helping MSMEs have easier access to many markets overseas, e-commerce is also helping MSMEs in scaling up through greater access to skilling, new and innovative technologies and affordable finance (Kumar, 2017).

India's Ranking

India has to focus on several areas in order to ensure that the country's nascent e-commerce sector lives up to its potential. India was ranked

low at 134th out of 176 economies in the ICT Development Index 2017, though slightly better than the 138th position in the previous year. The country needs to register major improvement in sub-indices including 'access' (fixed-telephone subscriptions, mobile-cellular telephone subscriptions, international internet bandwidth per Internet user, households with a computer and households with Internet access), 'use' (individuals using the Internet, fixed broadband subscriptions and active mobile-broadband subscriptions) and 'skills' (mean years of schooling, gross secondary enrolment, and gross tertiary enrolment) to ensure a higher rank (ITU, 2017).

Another important criterion for boosting e-commerce is the emphasis on policies that can promote cloud computing. In a ranking of 24 leading IT economies on such policies including on data privacy, security, cybercrime, Intellectual Property Rights (IPR), support for industry-led standards and international harmonisation of rules, free trade promotion, IT readiness and broadband deployment, India was ranked 20th in 2018. The country's ranking slipped from 18th in the previous edition in 2016 mainly due to perceived problems related to 'data privacy' ('lack of a personal data breach notification law'), and 'IT readiness and broadband deployment' ('failing to achieve original objectives of increasing broadband subscription in the country'), according to the assessment carried out by the global software industry body BSA (BSA, 2018).

India was ranked 80th out of 151 economies by the 2018 UNCTAD B2C E-commerce Index, which 'measures an economy's preparedness to support online shopping' on parameters including the share of individuals using the Internet, share of individuals with an account at a financial institution or with a mobile-money-service provider, secure Internet servers and postal reliability. India was ranked 83rd in 2017 (UNCTAD, 2018).

While India has marginally improved from its 2017 rank, the country has to expedite its efforts in all the above-mentioned parameters with the combined help of stakeholders including the industry, regulatory bodies, policy makers, civil society organisations and consumers in order to be digitally prepared for foreign trade and to take part meaningfully in global rule-making on e-commerce. Owing to the trend of increasing digital content in exports to cater to the demand for such products (as well as digital services), an inability to digitise manufacturing could hurt the competitiveness of a country's exports globally, while greater digital content could add value to a country's exports. Thanks to its expertise in digital services including telecommunications and computer programming and related services, India is among the leading countries globally in terms of value-added by digital services to total exports. However, the scenario is not the same when it comes to manufacturing. It would, therefore, be important for India to take necessary steps including in its policies related to manufacturing and exports in order to increase the digital content in its overall exports, especially considering that it lags behind several developing and developed countries in that aspect (Banga, 2018).

Growth and Concerns

The rapid growth of the e-commerce sector in India is due to an increase in the number of users of smart phones and internet, rise in investments, and a jump in the number of active e-commerce companies as well as the brick and mortar retail companies selling their products and services online in addition to the offline route.

However, this has also led to the concerns of its possible adverse impact on the brick and mortar retail trade, especially on the Micro, Small and Medium Enterprises (MSMEs) segment. India's traders' body, the Confederation of All India Traders (CAIT), has alleged that FDI in

e-commerce could lead to the country's retail trade being controlled and dominated by the global e-commerce giants. The availability of finance for the global e-commerce players at much lower rates when compared to the local MSMEs makes the playing field uneven for the Indian firms, the CAIT has said (CAIT web link on e-commerce).

The anti-monopoly watchdog Competition Commission of India (CCI), in a study, has found that at the heart of several issues that cropped up in its market study was the "bargaining power imbalance and information asymmetry between e-commerce marketplace platforms and their business users." While not formally determining if any of those practices amount to infringement of the provision of competition law, the CCI recommended that "improving transparency over certain areas of the platforms' functioning can reduce information asymmetry and can have a positive influence on competition outcomes." On the issue of deep discounts offered by digital platforms, the CCI said while it is "seen as a means to establish network effects for user on-boarding", such discounts "can harm competition when used as an exclusionary device by enterprises with market power" (CCI, 2020a).

The CCI has also directed an investigation into "whether the alleged exclusive arrangements, deep-discounting and preferential listing" by e-commerce companies such as Flipkart and Amazon "are being used as an exclusionary tactic to foreclose competition and are resulting in an appreciable adverse effect on competition" in violation of the provisions of the Competition Act (CCI, 2020b).

ITA Experience

Another factor that has to be considered is India's experience after joining the WTO's original Information Technology Agreement (known as ITA-1) in March 1997. The ITA is a plurilateral agreement under which the signatory countries have agreed to eliminate tariffs on IT products covered by the pact. Due to India's "discouraging" experience with the ITA-1, India decided not to be part of the expanded ITA (known as ITA-2) (Govt. of India, 2015).

The tariff cuts following the ITA-1 to zero or close to zero tariff led to an increase in IT imports into India, and did not boost innovation and local manufacturing of electronic items despite a huge domestic market. Domestic manufacturing faced constraints including poor infrastructure, complex regulation, lack of facilities such as power and water, Besides, India's robust IT services sector, chip design sector and Research and Development (R&D) had global connections, but did not have strong links with the local electronic manufacturing sector. All these factors led to a rise in imports from countries including China, Japan and South Korea. China, on the other hand, gained substantially from the ITA-1 and emerged as a leading manufacturer and exporter of IT products thanks to its innovation policy, huge investments in R&D, and initiatives taken to boost high-tech exports (Ernst, 2016).

Therefore, India should not focus merely on developing or supporting national e-commerce platforms to boost e-commerce. If such a platform does not feature Indian products with high digital content or digital services by domestic firms, Indian consumers could go for products with high digital content or digital services offered on that platform by business entities from other countries. Therefore, the proposed National E-commerce Policy has to be comprehensive with close links to the objectives of other policies meant for development of industries, local manufacturing, technology and skills as well as for modernising digital infrastructure and boosting exports. India should also study the e-commerce rules and ecosystem in China, which has now become a leading e-commerce economy in the world (See Box 4.1).

Box 4.1: Perspectives from the Chinese Model

The size of China's digital economy is around 33 per cent of its GDP in 2017 (up from 15 per cent in 2008), as against 20 per cent in India, Brazil and South Africa and 59 per cent in the U.S. The digital economy in China is estimated to touch around 50 per cent of the GDP by 2025. Digitalisation is being supported through government policies including those promoting innovation. China started with a 'light touch' regulatory regime in the early years of digitalisation, before gradually bringing out stringent norms such as the ceiling on online money transfers. Currently, issues including consumer protection, cross-border data transfer, data privacy, competition laws, anti-money laundering and cyber security are covered under the regulatory regime. Also helping China is its 700 million internet users (including over 280 million people below 25 years of age), and a large number of MSMEs. The country has emerged as a leader in e-commerce (accounting for more than 40 per cent of global transactions) and fintech (accounting for more than 70 per cent of the overall global valuations). It has global giants like Alibaba in e-commerce platforms and cloud computing, as well as Alibaba (Alipay) and WeChat Pay in e-payments. These companies have generated millions of jobs (including Alibaba creating over 30 million jobs and Didi taxi platform linking 13 million drivers). Also being witnessed is the trend of replacing low-skilled workers with robots, like in the case of Foxcon that did away with 60,000 workers and deployed 40,000 robots. China is also a leading venture capital investor in technologies such as 3D printing, virtual reality, artificial intelligence, robotics and autonomous driving (Zhang and Chen, 2019).

China was instrumental in taking forward the initiative under G20 to define 'digital economy' as "a broad range of activities that include using digitalised information and knowledge as the key factor of production, modern information networks as an important activity space, and the effective use of ICT as an important driver of productivity growth and economic structure optimisation." In China's digital sector, manufacturing production has the upper hand with it accounting for 55 per cent of the overall value of the country's ICT sector as against the contribution of the services sector at 45 per cent. Another feature of China is the greater digitalisation seen in urban areas as compared to that in the rural regions (García-Herrero and Xu, 2018). China has also seen villages being transformed thanks to the spread of e-commerce (as seen in the case of "Taobao villages" - named after the Alibaba Group-run online shopping platform - where a minimum of 10 per cent of households are involved e-commerce activities (World Bank, 2016). E-commerce started in China in 1996, and the growth of the sector started accelerating from 2000. In 2007, the government came up with an "E-commerce Development Five-Year plan" to give a boost to the sector. This was followed up with "E-commerce model specification" and "online shopping service standard" in 2009. The People's Bank of China in 2011 gave its nod to 27 enterprises for payment transactions. In 2014, most provinces in China executed a strategy for cross-border development of e-commerce to help Chinese companies go global. The major target economies for China's E-commerce sector include the U.S., the European Union, ASEAN countries, Japan, Russia, South Korea, Brazil and India (Hongfei, 2017).

Owing to an increase in online shoppers in China, its e-commerce imports have also showed growth. China, as of 2016, has 13 cross-border e-commerce comprehensive 'pilot' cities. The major Chinese cross-border e-commerce players include DHgate, Alibaba International Website, AliExpress, Wish, Winliner (all five e-commerce export platforms), DX, LightInTheBox, Osell, Milanoo (all four e-commerce export retailers), Global Taobao, Ebay, Tmall International, Ymatou (all four e-commerce import platforms), Amazon (overseas), JD (overseas) and Jumei (all three e-commerce import retailers). Shaji, a town in China, has grown to become a leader in furniture thanks to e-commerce and government support. In addition, e-commerce companies like Alibaba, JD and Lecuntao are now into supporting rural areas in e-commerce (International Trade Centre, 2016).

Source: Author's compilation from Zhang and Chen, 2019; García-Herrero and Xu, 2018; World Bank, 2016; Hongfei, 2017; and International Trade Centre, 2016.

On realising the growing importance of e-commerce and to boost tax revenues by including e-commerce participants in the tax net, the Budget 2020-2021 had proposed deduction of TDS (Tax Deducted at Source) by e-commerce operators on "all payments or credits to e-commerce participants (a resident of India selling goods and/or providing services, or in other words, third-party sellers on the platforms of an e-commerce operator) at the rate of 1 per cent in PAN (Permanent Account Number)/Aadhaar cases and 5 per cent in non-PAN/Aadhaar cases". The tax will have to be deducted on the gross amount of sale of goods and/or services. However, there was a provision aimed at providing relief to small third-party sellers on e-commerce platforms, as it was proposed to exempt an individual and HUF (Hindu Undivided Family) receiving less than Rs. 500,000 and furnishing PAN/Aadhaar number (Govt of India, 2020).

The Government has also taken note of allegations that e-commerce players were indulging in anti-competitive practices including deep discounting and predatory pricing. It has brought in clarifications and some changes to provisions relating to e-commerce in the FDI policy.

Currently, 100 per cent FDI under automatic route is allowed in marketplace model (where the e-commerce player provides an information technology platform on a digital and network to be a facilitator between buyer and seller) of e-commerce. FDI is not permitted in inventory model (where the e-commerce entity owns all the inventory of goods and services and then directly sells them to the consumers) of e-commerce. As per the amended FDI norms, e-commerce marketplace entities will have to submit to the Reserve Bank of India (annually by 30 September for the preceding financial year) a certificate along with a report of statutory auditor that they have complied with all the guidelines including the conditions specified in the FDI policy. The government had also clarified that though there is "no distinction between the taxation regimes of Indian and foreign e-commerce companies as such", the differences in the taxation regimes applicable to domestic and foreign companies are also relevant to the e-commerce sector. Also applicable is the Equalisation Levy - a flat 6 per cent tax on 'the revenue derived by a non-resident multinational enterprise, which is not physically present in India, but is providing digital advertising services to Indian customers' (Govt. of India, 2019d).

E-commerce Policy and the Related Issues

In February 2019, the government released a draft National E-commerce Policy with links to flagship schemes such as 'Make in India', 'Digital India', 'Skill India', 'Smart Cities' and 'Startup India'. The strategy included measures on data localisation to ensure local/sovereign ownership and control of data generated within the country, curbs on cross-border data flows, promotion of MSMEs, startups and e-commerce exports, in addition to steps for ensuring consumer protection. It talks about development of data-storage facilities/ infrastructure and promotion of domestic alternatives of foreign-based cloud services and email facilities. Besides, it prescribes anti-counterfeiting measures as well as calls for integration of RBI, Customs and India Post systems to enhance tracking of imports through e-Commerce. According to the draft policy, the categories of data exempted from restrictions on cross-border data flow include: "(i) data not collected in India; (ii) B2B data shared between business entities under a commercial contract; (iii) data flows through software and cloud computing services (having no personal or community implications); and (iv) data (excluding data generated by users in India from sources like e-commerce platforms, social media activities, search engines) shared internally by multinational companies" (Govt. of India, 2019e).

India's data localisation norms are spelt out in policies including the National Telecom M2M Roadmap, the RBI notification on 'Storage of Payment System Data', the Unified Access License, the Companies Act, 2013 and its Rules, the FDI Policy 2017 and the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, besides in (draft) policies including the draft e-commerce policy, draft e-pharmacy regulations and Personal Data Protection Bill 2019 (see Box 4.2).

Box 4.2: Salient Features of the Personal Data Protection (PDP) Bill, 2019

The PDP Bill has been introduced in Parliament (Lok Sabha) (Govt. of India, 2019f). The Bill, among other objectives, aims to protect rights, including privacy, of individuals ('data principal') regarding their *personal data*, norms on transfer of such data across borders as well as to set up a Data Protection Authority of India for the same purposes. It covers 'data fiduciaries' including the government and its agencies, Indian companies and foreign firms handling personal data. It categorises data into personal data, sensitive personal data and critical personal data. It defines "*sensitive personal data*" as meaning to include personal data related to '(i) financial data; (ii) health data; (iii) official identifier; (iv) sex life; (v) sexual orientation; (vi) biometric data; (vii) genetic data; (viii) transgender status; (ix) intersex status; (x) caste or tribe; (xi) religious or political belief or affiliation.'

The Bill specifies that consent (which is free, informed, clear and capable of being withdrawn) shall be explicitly obtained by the data fiduciary from the data principal in respect of processing of any sensitive personal data and only for clear and lawful purposes. It does not specifically define "critical personal data", but terms it as 'personal data as may be notified so by the Central Government'. It also states that 'critical personal data shall only be processed in India'. However, sensitive personal data can be transferred outside India for processing but only after the data fiduciary meets certain conditions including obtaining explicit consent from the data principal for such transfer.

The Bill also states though sensitive personal data may be transferred outside India on meeting the specified conditions, 'such sensitive personal data shall continue to be stored in India'. The rights of the data principal specified in the Bill include the right to obtain confirmation (regarding processing of personal data) and access, right to correction (of incomplete, inaccurate and out-of-date personal data) and erasure (of such data, data no longer needed and in cases where the data subjects withdraws consent), right to data portability and right to be forgotten. As per the Bill, the data fiduciaries will also need to have periodically reviewed and updated security safeguards, an effective grievance redressal mechanism, 'privacy by design' policy and, in specified cases, carry out 'data protection impact assessment'. The Bill also states that 'data principal may give or withdraw his consent to the data fiduciary through a consent manager' (who is a 'data fiduciary' registered with the Authority and 'enables a data principal to gain, withdraw, review and manage their consent' through a platform that is 'accessible, transparent and interoperable'). The Bill proposes to empower the Central Government to exempt any government agency from the application of the legislation for protecting national security, sovereignty, for ensuring public order and to maintain friendly ties with foreign States. It also empowers the Central Government (in consultation with the Data Protection Authority) to direct "any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government." It specifies that the proposed Authority 'shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations' under the legislation. The Bill also has norms on 'social media intermediary' ("an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services", but not including those primarily enable 'commercial or business oriented transactions, or provide access to the Internet, or are 'in the nature of search-engines, on-line encyclopedias, e-mail services or online storage services'.) Penalty of upto Rs 15 crore ('or four per cent of the data fiduciary's total worldwide turnover of the preceding financial year, whichever is higher') can be imposed on data fiduciary violating certain provisions of the legislation (Govt of India, 2019g). The Bill has been referred to a Joint Committee of the Houses of Parliament (Govt of India, 2019h).

Source: Govt of India, 2019 f, g, h.

The objectives of these policies, among others, include promotion of innovation and enhancing national security. The local industry is divided. Some big companies are supporting data localisation policies saying they would ensure data protection and help them to set up their own data centers. On the other hand, small firms and startups are opining that these policies would increase their compliance costs. However, there are concerns over India's capabilities to ensure compliance, and over its infrastructure and safeguards that are necessary to support the localisation norms. Besides, there are apprehensions that these moves would adversely impact India's trade with several countries. The question now is whether it is better to pursue an alternate strategy of negotiations and consensus at the global level including at the WTO on matters that concern India and the developing world at large. Also, there are suggestions that instead of brining in broad data localisation norms, India could consider restricting them to certain sectors of its interest. Besides, as part of a trade agreement, India could look at allowing cross-border data transfer on conditions such as the partner country (or countries) having similar norms including on privacy (Basu *et al.,* 2019).

Several stakeholders including business organisations, law firms, think-tanks and consultancy firms responded to the government's draft e-commerce policy. Industry body **NASSCOM** has raised concerns over the broad definition of e-commerce as it includes everything related to the digital economy (buying, selling, marketing or distribution of goods, including digital products and services; through electronic network). Interpreting that the inclusion of the term 'marketing or distribution' within the definition of e-commerce could be to align the definition with the WTO, NASSCOM, however, pointed out that the proposed definition in the draft e-commerce policy differs from that given in the FDI Policy, 2017 as well as the Consumer Protection Bill, 2018 (in which the definition is similar). NASSCOM has suggested that the policy should limit its scope to e-commerce as defined in the FDI Policy, 2017 to ensure regulatory clarity, without adversely impacting India's participation in e-commerce talks at the WTO. On the policy proposal of seeking disclosure of source code with a view to facilitate transfer of technology and development of applications for local needs as well as for security, NASSCOM said that such a move could result in businesses delaying introduction of technology in India. It said: "Technology transfer is usually facilitated through policies which encourage cross-border trade, FDI, joint ventures, licensing agreements, international movement of people and government to government co-operation. Technology transfer is more likely to happen in conditions which afford greater protection to intellectual property (IP) than those that mandate disclosure of source code." Regarding restrictions on cross-border data flows mentioned in the draft policy, NASSCOM said such a move could create trade barriers. NASSCOM said enabling cross-border flow of data generated in India would lead to creation of diverse datasets, which in turn reduces the risk of biases and ensures greater accuracy in results, particularly in sectors that depend on predictive analytics like healthcare and agriculture. Besides, business entities would find it difficult to use Artificial Intelligence-based solutions (which also need large datasets) in India and address several important developmental issues (NASSCOM, 2019).

New Delhi-based not-for-profit organisation **Digital Empowerment Foundation** argued for harmonisation of the policy with highest available standards of rights-protective data protection principles and frameworks to ensure economic growth and development along with economic and social justice to individual citizens (Digital Empowerment Foundation, 2019). On the issue of cross-border data transfer, **US-India Strategic Partnership Forum (USISPF),** a non-profit organisation

aiming to boost the U.S.-India ties, said India should seek to ensure interoperability with globally recognised privacy frameworks, such as the European Union's General Data Protection Regulations (GDPR) and the APEC privacy principles, in which consent of the data principal is the main criterion used to process sensitive personal data. Arguing that 'sovereign rights are extended over power and ability to act, not over citizens, resources or data', the USISPF said, therefore 'the State cannot, by the very nature of the right, have sovereign rights over data' (USISPF, 2019).

Video industry trade body **Asia Video Industry Association (AVIA)** also took up this issue by pointing out that the proposed policy's view that 'data should be a national resource controlled by the government' seems to be in conflict with the Personal Data Protection Bill, 2018 'desire to empower Indian citizens to own and control their own data'. The AVIA wanted clarity on the matter. On the inclusion of "marketing or distribution" into the definition of e-commerce, the AVIA said the proposed policy has expanded the scope of e-commerce 'beyond online retailing to cover the entire digital economy, including sectors such as BPOs, ISPs, digital payments, the content ecosystem, search engines, and the entire Indian IT Industry.' Pointing out that these sectors are governed and regulated by various statutes such as the IT Act and the Consumer Protection Act and regulators such as the RBI and Competition Commission of India, the AVIA said such a broad definition of e-commerce would 'disrupt the regulatory harmony in India's digital sector and undermine the proposed initiatives of other line Departments/Ministries to streamline cross-sectoral regulations/legislations on issues such as data protection (Personal Data Protection Bill, 2018- now 2019) and consumer protection (Consumer Protection Bill, 2018 now Consumer Protection Act, 2019)'. Another issue is that currently Online Curated Content (OCC) services that 'provide content through subscription services (and not permanent download of digital goods as replacement to physical goods)' are not covered under the definition of e-commerce in the Consolidated FDI Policy of India, as per the AVIA. Currently, according to an interpretation of the FDI Policy, FDI upto 100 per cent is allowed in OCC services under the automatic route, subject to applicable laws/regulations, security and other conditionalities. Referring to this, the AVIA stated that a broad definition of e-commerce that includes 'marketing or distribution' could result in 'the application of India's restrictive FDI policy on e-commerce goods retailing to the entire digital sector, including digital services where 100 per cent FDI is currently permitted through the automatic route [Chapter 5.2(a) of the Consolidated FDI Policy, 2017].' Therefore, the AVIA wanted the proposed policy to remove such ambiguities and unintended consequences (AVIA, 2019).

The country's broadband sector policy forum and think-tank **Broadband India Forum (BIF)** pointed out that there was no empirical evidence to support the claim that data localisation measures would improve data security. Besides, India being a power deficit country, would find it difficult to manage the enormous amount of power that would be required by data centers to store the data generated within the country, it stated. The BIF also cautioned that curbs on cross-border data flows could lead to retaliatory measures from other countries that could hurt the prospects of India's IT/ITeS sector and economic growth and even the startups in India. It also sought harmonisation of the views in the proposed e-commerce policy with the legislation on personal data protection (currently only a Bill) on issues including consent, data sharing and cross border data flows. It was also against the mandatory requirement of disclosing source code (BIF, 2019).

The **Global Services Coalition (GSC)**, representing the services sector in countries including Australia, Canada, Europe, Hong Kong, Japan, Taiwan and the UK on issues

relating to international trade and investment, called for a clear definition of what constitutes sensitive data. Terming data flows as the building blocks of technologies including the Internet of Things, cloud computing, Artificial Intelligence and those other services and technologies coming up in the context of the Fourth Industrial Revolution, the GSC expressed concern over the proposed restrictions on data movement. The industry body said legitimate public policy objectives including those concerning data security and personal data protection should be achieved without curbing cross-border data. It added that all exceptions should be non-discriminatory and in compliance with the General Agreement on Trade in Services (GATS) provisions. On the issue of mandatory disclosure of source code with a view to facilitate transfer of technology and developing applications for local needs as well as for security, the GSC said such provisions could adversely impact investment inflows into India in services sectors including financial technologies. Besides, the GSC recommended that instead of relying on data localisation requirements to address its data privacy and security concerns, India could consider a regime similar to the APEC Cross-Border Privacy Rules that incorporates a voluntary set of privacy principles to guide data protection practices and procedures. It added that in order to govern cross-border data transfers, countries such as Singapore, Australia and Japan, which are among the leading markets for digital technologies, products and services, have legal processes such as accountability, consent, binding corporate rules and contractual clauses (GSC, 2019).

On the issue of the draft policy exempting 'data flows through software and cloud computing services (having no personal or community implications)' from the restrictions on cross-border data flows, consulting firm **Albright Stonebridge Group** sought greater clarity stating that "it is unclear whether any data can literally have 'no personal or community implications'." On the proposed policy mandating businesses to share data with the Indian government in certain cases as well as with Indian firms including startups, the consulting firm said such "requirement to share data - particularly with competitors - is not just onerous but risks discouraging investment and innovation, and significantly undermining competition on the merits." On the proposed policy requirement of "sharing of 'community data' that serves larger public interest (subject to addressing privacy-related issues) with start-ups and firms", Albright Stonebridge Group wanted the term 'community data' to be defined precisely (ASG, 2019).

Global software industry body **BSA** referred to the proposed e-commerce policy's take on anonymised data and suggested exempting anonymised data from its coverage. According to the draft policy, "even after data is anonymised, the interests of the individual cannot be completely separated from it. Data about a particular group will always have something of value for them." BSA cited the definition of anonymised data in the Personal Data Protection Bill, 2018 as "data that is not reasonably linkable to a specific individual," and stated that going by that definition 'such data is not personal and therefore does not implicate individual privacy'. It further said excluding anonymised data from the purview of the policy would 'encourage wide-ranging innovative uses of data beneficial to all forms of Indian firms and users'. The BSA objected to the proposed policy provision prohibiting business entities from sharing sensitive data with a third party 'even with customer consent'. It said "respecting individual autonomy means that individuals should be able to control and share their personal information as they wish. By prohibiting an individual from consenting to specific uses of his or her data, the Policy would be inconsistent with the underlying purpose of a data protection regime" (BSA, 2019).

The non-profit organisation and research body **Centre for Internet and Society (CIS)** objected to inclusion of anti-piracy measures

in the draft e-commerce policy. The CIS said combating piracy is already a part of the Indian Copyright Act, 1957 and, therefore, is in the domain of intellectual property law and enforcement. The CIS also countered the draft policy treating data generated in India purely as a national resource by stating that 'overlooking privacy as a fundamental right' and focusing more on the aspect of data as a national resource can unintentionally enable the public and private sectors to carry out exploitative practices in a manner that 'undermines individual dignity and autonomy and replicates existing practices that can be seen globally'. It also wanted the draft policy to lay greater emphasis on security and specify how e-commerce services will have to comply with the prevailing security frameworks and standards in addition to encouraging improvements in the existing security frameworks (CIS, 2019).

India is among the world's leading countries in terms of e-commerce market and data generation. It also has a vast pool of skilled workers and youth. In order to use these factors to its advantage and since economic activity in the future is expected to follow data, the proposed policy has taken the approach of retaining control of data to ensure job creation within India in sectors such as cloud computing and data analytics. The policy aims to facilitate the development of data-storage facilities/ infrastructure in the country through measures such as granting them 'infrastructure status' and promote domestic alternatives of foreign-based cloud services. The expectation is that these measures will result in local employment generation. Going forward, the government should also consider that restrictive norms could attract retaliatory measures from other countries. Besides, it would be important to take into account a scenario where the digital divide at least within India is narrowed, and when Indian enterprises scale up and develop ambitions to expand their footprints in various markets overseas including in poor countries.

Views and Suggestions Regarding Some Core Aspects

The views and suggestions in Box 4.3 are based on stakeholder consultations on the position taken by India on various issues and what is considered pragmatic in the long-term interest of the country.

Box 4.3: Views and Suggestions

Definition:

Draft Policy (Govt. of India, 2019d) **:**

Definition: 'E-commerce' and 'digital economy' used interchangeably; includes buying, selling, marketing or distribution of (i) goods, including digital products and (ii) services; via electronic network. Page 9 of the draft.

Views:

The policy aims to cover the entire digital economy, thereby going beyond its scope of just e-commerce comprising online retail transactions. This amounts to regulatory over-reach, resulting in ambiguities, uncertainty and regulatory overlaps.

In the FDI Policy 2017, e-commerce is defined as 'buying and selling of goods and services including digital products over digital and electronic network'. This excludes the term 'marketing or distribution' (Govt. of India, 2017). Even the definition of e-commerce (buying or selling of goods or services including digital products over digital or electronic network) under the Consumer Protection Act, 2019 is similar (Govt. of India, 2019i). However, WTO defines it as the "production, distribution, marketing, sale or delivery of goods and services by electronic means". According to the WTO, an e-commerce transaction can be between enterprises, households, individuals, governments and other public or private organisations (WTOe).

Box 4.3 continued...

Box 4.3 continued...

Suggestions:

The scope of the policy and definition should be limited to e-commerce. The definition of e-commerce across all regulatory regimes in India should be the same. Care should be taken to ensure that it does not impact India's position at the WTO on e-commerce talks.

Also, though the policy refers to 'sensitive data' and 'personal data', these terms are not defined. The policy needs to ensure consistency in this regard with other concerned laws including on Personal Data Protection.

Data localisation / curbs on cross-border data flows:

Draft Policy (Govt. of India, 2019d) **:**

Conditions are required to be adhered to by business entities which have access to sensitive data of Indian users stored abroad. Sharing of such data with third party entities, even with customer consent, is barred under the Policy. Violation of conditions of this Policy will be made accountable to prescribed consequences (as formulated by the Government of India). Page 6 of the draft.

At this juncture there is no legal framework that would permit the government to impose restrictions on cross-border flow of data. Without having access to the huge trove of data that would be generated within India, the possibility of Indian business entities creating high value digital products would be almost nil. Domestic technology companies would be merely processing outsourced data work. Further, by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country. Page 15 of the draft.

A legal and technological framework to be created that can provide the basis for imposing restrictions on cross-border data flow from the following specified sources:

a) Data collected by IoT devices installed in public space; and

b) Data generated by users in India by various sources, including ecommerce platforms, social media, search engines etc.

The legal and technological framework would also provide basis for sharing the data collected by IoT devices under (a) above with domestic entities for use in research and development for public policy purposes. Page 16 of the draft.

A business entity that collects or processes any sensitive data in India and stores it abroad, shall be required to adhere to the following conditions: a) All such data stored abroad shall not be made available to other business entities outside India, for any purpose, even with the customer consent; b) All such data stored abroad shall not be made available to a third party, for any purpose, even if the customer consents to it; c) All such data stored abroad shall not be made available to a foreign government, without the prior permission of Indian authorities; d) A request from Indian authorities to have access to all such data stored abroad, shall be complied with immediately; e) Any violation of the conditions mentioned above shall face the prescribed consequences (to be formulated by the Government). Page 16 of the draft.

Location of the computing facilities like data centers and server farms within the country will not only give a fillip to computing in India but will also lead to local job creation. Page 16 of the draft.

A time-frame would be put in place for the transition to data storage within the country. A period of three years would be given to allow industry to adjust to the data storage requirement. Page 18 of the draft.

In light of the increasing importance of data protection and privacy, the National e-Commerce Policy ("Policy") aims to regulate cross-border data flow, while enabling sharing of anonymised community data (data collected by IoT devices installed in public spaces like traffic signals or automated entry gates). Page 6. Suitable framework will be developed for sharing of community data that serves larger public interest (subject to addressing privacy-related issues) with start-ups and firms. The larger public interest or public good is an evolving concept. The implementation of this shall be undertaken by a 'data authority' to be established for this purpose. Page 17 of the draft.

Box 4.3 continued...

Box 4.3 continued...

Views:

Mandating localisation of all kinds of data and a blanket ban on cross-border data flows - on the grounds of employment generation, data security, ensuring a level playing field between local and foreign firms and law enforcement - especially without adequate proof to back these claims, could act as a deterrent for foreign investment and Research and Development as well as a trade barrier.

It could lead to higher costs for businesses to operate in India and comply with these regulations as well as an entry barrier to foreign firms. This would, in turn, adversely impact innovation, scaling up of start-up ecosystem, job creation, development of cloud service providers and ease of doing business in the country.

It could also result in inferior goods and services. The higher compliance costs, including those associated with storing data in India, would hurt the operations of startups and micro, small and medium enterprises more than the big firms with deep pockets. Moreover, restrictions could lead to retaliatory measures from other countries.

Besides, storage of personal data in servers situated in a few sites in the country could instead make them more vulnerable to attacks when compared to data storage in multiple locations including outside India.

Firms in several sectors including health, banking, automobiles, information technology, energy and retail would need to collect personal data and then use advanced technologies such as data analytics and artificial intelligence to develop products and services customised to certain individual or common requirements or for improving the quality of their products and services.

Many of these companies, including the listed ones, adhere to global best practices including on data ('data responsibility' principles – including on data ownership, privacy, access, flows, sharing, security and mobility) and corporate governance (IBM, 2017; Daimler, 2019; Iberdrola, 2018).

If blanket curbs are imposed on data flows, it would reduce the size, diversity and quality of datasets and in turn impact the accuracy of findings in several important sectors including medical care due to the gaps in data. This could increase the risks of medical errors and even result in deaths. Restricting flow of data across borders can also lead to delays in responding to natural disasters. On the other hand, seamless flow of data across borders can lead to better globally networked operations in sectors including textiles and clothing, retail, insurance, micro-lending and shipping. It can improve cyber security and fraud prevention (BSA, 2017).

It should be noted that in the Puttaswamy Judgement [Justice K.S. Puttaswamy (Retd.) and Another. v. Union of India and Others., (2017) 10 SCC 1], the Supreme Court of India had recognised the right to privacy as a fundamental right of Indian citizens subject to certain reasonable restrictions, and the notion that an individual has the control and ownership over his/her data.

Data flow restrictions in the draft e-commerce policy also seem to be contradictory to the Personal Data Protection Bill, 2019 that proposes to enable cross-border personal data transfer on meeting specific conditions, including obtaining consent of data principal for data transfer outside India.

Besides, the curbs could be in violation of GATS Article XIV (c) which specifies that measures to secure compliance with laws or regulations including those regarding the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts are "subject to the requirement that (they) are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services" (WTOb).

Another issue is regarding data that is aggregated and anonymised. Such de-identified personal data, for instance, in sectors like health, could lead to innovative public health solutions. However, there are risks including that of the possibility of retracing and re-identifying the individuals concerned in this anonymised data. There are studies globally regarding this issue and on the possible measures to prevent such re-identification. (Wes, 2017; Narayanan and Felten, 2014; Cavoukian and Castro, 2014). The policy also rightly notes that "even after anonymisation, the interests of the individual cannot be completely separated from the derivatives that may be obtained by analyzing and drawing inferences from a certain set of data."

Box 4.3 continued...

Box 4.3 continued...

Suggestions:

The national e-commerce policy should be in line with the legislations on Personal Data Protection, Consumer Protection, Information Technology, Competition etc., and incorporate detailed provisions related to 'data responsibility' in a manner that would avoid complexities and conflicts with other policies/laws/rules.

The policy should also consider enabling consumers to move their data from one service provider to another, while ensuring that in such a case the personal details regarding consumers seeking data portability are deleted from the service provider that he/she seeks to leave. This would enhance competition and ensure that service providers and goods manufacturers constantly improve their services and goods. The norms in this regard can be based on the EU GDPR, which enforces this right to data portability.

The policy could also include norms to enable the Indian Government to enter into pacts with partner countries on the lines of the EU-US Privacy Shield Framework, where transfer of personal data from EU to the US – i.e., to firms certified in the US under the Framework – was agreed upon in return for the US ensuring privacy protection of EU citizens to EU standards (including norms on what would constitute adequate level of data protection). However, it is important to firm up an 'adequacy mechanism' on the lines of EU GDPR with powers to authorities to determine an 'adequate' level of data protection. Also, India and the partner country with which it enters into such a reciprocal pact for data access would need to have stronger institutional capacity to monitor firms and enforce compliance with the framework's norms. In this regard, it would be vital to for India to have a strong cyber security framework including on encryption.

In cases of any data breach as well as to avoid such incidents, the policy can consider the provisions on notification of breach in the EU GDPR and the security safeguard provisions in the APEC Privacy Framework (This framework aims for effective privacy protection, but avoids being a barrier to information flows so that it can facilitate trade and promote economic growth. It is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data). Also relevant in this regard is the APEC Cross-Border Privacy Rules (CBPR) System that implements the APEC Privacy Framework. In order to ensure personal data protection, the CBPR not only has provisions empowering consumers but also norms on cross-border enforcement cooperation. (APEC, 2019).

Besides, instead of mandating all kinds of data to be stored in the country, the policy should specify the kinds of data (eg: payment data, health-related data, community data) that needs to be locally stored by giving detailed reasons for the same, and those data that would be exempt from localisation. However, it is important to first carry out a study of costs and benefits of data localisation measures on various sectors and the impact of such measures on the Indian economy. Some studies have found that forced data localisation laws lead to greater costs for companies and would fail in achieving its objectives (Leviathan Security Group, 2017; Cory, 2017).

Given the wide-ranging implications including on privacy and security, there is a need for greater stakeholder consultations on several issues including in developing a framework for concepts like 'community data' and 'anonymisation of data'. Similarly, given the numerous objections from the industry and the mixed reactions to data localisation measures, there is a need for further consultations to find a middle path on issues such as fixing a time period that would be provided to the industry to comply with the data storage requirement norms. Also, it is important to ensure that such a time period, if deemed necessary, is consistent across legislations.

Box 4.3 continued...

Box 4.3 continued...

Disclosure of source code:

Draft Policy (Govt. of India, 2019e) :

During (WTO) negotiations, policy space must be retained to seek disclosure of source code for facilitating transfer of technology and development of applications for local needs as well as for security. Page 10 of the draft.

Views:

The draft policy does not provide evidence to back the claim that disclosure of source code, considered a kind of trade secret, would facilitate transfer of technology and development of applications for local needs as well as for security. A blanket requirement for source code disclosure for all sectors could hurt foreign investment inflows, technology transfer and innovation, especially since foreign firms want a stronger intellectual property rights regime. Another issue here is the security risks associated with the centralised storage of source codes of firms, which in turn could hurt the business confidence in case of a security breach.

Suggestions:

Instead of a mandatory disclosure of source code in all sectors, the government, while assuring protection of intellectual property rights of firms, should come up with a positive list approach. In such a move, it should detail the critical infrastructure / sensitive sectors where such disclosure would be mandatory by giving the reasons including those relating to security concerns and where technology transfer is considered essential as well as for the purposes of public procurement or in the case of abuse of monopoly position. All the norms should be consistent with India's commitments at the WTO, investment agreements and the country's IPR policy. As an alternative solution, the government should carry on its activities including its 'Policy on Adoption of Open Source Software' to promote the use of Open Source Software technologies. In addition, the policy needs to incorporate details on what the Government would do once it gets access to source codes and the associated Intellectual Property Rights.

Moratorium on customs duty:

Draft Policy (Govt. of India, 2019e) :

India has thus far not been a party to negotiations on e-commerce at the multilateral level. The push for initiating negotiations on substantive obligations related to e-commerce includes elements like permanently accepting the moratorium on imposing customs duties on electronic transmissions. By agreeing to the permanent moratorium, countries which have tariff schedules, which allow putting duties on these kinds of products, will give up these rights and lose revenues. Assuming that all non-agriculture products can be traded electronically, then everything will be traded at zero duty. So, the protection that is available to India, for the nascent industries in the digital arena will disappear at once, and that is an immensely important issue which concerns public policy makers in the developing world. Page 10 of the draft.

It has been globally accepted that there is a need to reconsider the traditional approach towards addressing the issues related to taxation. India has been quick to adjust to these changes. For instance, the concept of 'significant economic presence' was introduced in the 2018 Budget. It is important to move to the concept of 'significant economic presence' as the basis for determining 'permanent establishment' for the purpose of allocating profits of multinational enterprises between 'resident' and 'source' countries and expanding the scope of 'income deemed to accrue or arise in India' under Section 9(1)(i) of the Income Tax Act, 1961. The current practice of not imposing custom duties on electronic transmissions must be reviewed in the light of the changing digital economy and the increased role that additive manufacturing is expected to take. A 2017 UNCTAD report suggests that it would be mostly developing countries which would suffer loss in revenue if the temporary moratorium on custom duties on electronic transmissions is made permanent. Page 27, 28 of the draft.

Box 4.3 continued...

Box 4.3 continued...

Views:

In February 2019, an UNCTAD study showed that the total potential tariff revenue loss (including physical imports and electronic transmissions) for high income countries (which are WTO Members) due to the moratorium (estimated at the aggregate level in 2017, and using average bound duties) is only USD 289 million. However, as against this, the total potential tariff revenue loss from moratorium for developing countries is to the tune of a whopping USD 10 billion (India's loss is valued at USD 497.2 million) (UNCTAD, 2019b). OECD reports show the challenges of taxing digital businesses as such corporate entities resort to tax avoidance strategies that take advantage of the loopholes in the laws by artificially shifting profits to low or no-tax havens (OECD, 2019c). Faced with this situation, several economies brought changes to their laws to raise tax revenues through GST or VAT or customs duties on digital products / services. [In India, the GST legislation in India currently covers e-commerce transactions. The norms mandate registration only for those e-commerce operators 'who are required to collect tax at source'. 'Suppliers of services, with turnover up to Rs. 20 lakh, making supplies through e-commerce platforms' are 'exempted from obtaining registration', as per the norms (Govt. of India, 2019j)].

Meanwhile, at the global level, G20 Finance Ministers and Central Bank Governors have agreed to take forward the ambitious work programme that aims to address the tax challenges arising from digitalisation (G20, 2019a).

At the WTO, India and South Africa cited the example of Indonesia amending its law in 2018 to impose customs duties on e-transmissions, and said therefore, imposing customs duties on e-transmissions may be technically feasible. In a joint paper, India and South Africa said 'the customs duty moratorium exists precisely because it is feasible to impose customs duties on such transmissions'. The paper said it is vital for countries to safeguard policy and regulatory space in the WTO to firm up their national digital industrial policies which match the level and pace of their digital development so that they can then build digital capacities to face the challenges of digital trade (WTO, 2019e).

Suggestions:

India and other developing economies should not completely disengage themselves from the e-commerce related discussions and developments at the WTO, especially when 76 of the 164 WTO members - accounting for close to half of the WTO membership and around 80 per cent of the world trade - have decided to launch negotiations on global rules on e-commerce.

Staying disengaged would prevent India and other like-minded nations from steering the course of these discussions and building a global digital trade framework to their advantage. To avoid any isolation at the WTO-level, developing countries should build capacity to prepare themselves to engage in technical discussions at a later stage at the WTO when there is consensus. They should also form new coalitions to protect their common interests.

Owing to the limitations in the existing WTO norms regarding the coverage of e-commerce transactions and the tendency of WTO negotiations to be protracted, several countries - including from the developing world and even some of the lower income nations - are opting for bilateral FTAs with specific chapters addressing all the above-mentioned issues regarding digital trade. It would be important for developing countries like India with a growing digital economy and exports to experiment with more e-commerce provisions in its bilateral agreements to facilitate such digital trade and protect their interests.

Conclusion

E-commerce is a sector with enormous potential to bring about inclusive growth and sustainable development. However, in order to achieve these goals, it is important for nations to address key concerns including the digital divide. They should also take a balanced approach regarding data protection and data sovereignty on the one hand and on the other, find ways to enable digital technologies to solve the various developmental challenges faced by countries, especially in the developing world.

Countries contributing to over three-fourth of global trade have begun efforts towards launching WTO negotiations on trade-related aspects of e-commerce, even as several developing economies, including India, are trying to put in place national policies and a comprehensive regulatory framework on e-commerce. Several free trade agreements already have provisions on e-commerce. These provisions address issues including those relating to data localisation (or norms pertaining to storing data within the borders of a country) and cross-border data flows (or norms allowing data transfer overseas – that is beyond the borders of a country). The critical issues here are protection of privacy, interests of consumers as well as national security. Since rules regarding these issues vary across nations, there are calls for ensuring harmonisation as well as for entering into quid pro quo pacts like the U.S. and EU on privacy and data transfer. The concept of free and open internet that includes free cross-border data flow assumes importance from the point of view of human rights, commerce, and even democratic norms, where restrictions on information flow would certainly be problematic. However, in order to ensure balance, there should be adequate policy space to protect individual privacy and national security, while taking measures to eliminate barriers to enable sustainable national and cross-border e-commerce that complies with policies including on competition and consumer protection. Discussions on rule-making on e-commerce at the national, bilateral, regional and global level are constantly evolving. The issue, however, demands urgency due to the laws failing to keep pace with the rapidly changing digital technologies and their impact on several aspects of the global economy including trade. India and other like-minded developing countries should also keep in mind that staying disengaged from e-commerce discussions and developments at the WTO would prevent them from steering the course of these discussions and building a global digital trade framework to their advantage. To avoid any isolation at the WTO-level, they should build capacity to prepare themselves to engage in technical discussions at a later stage at the WTO when there is consensus. They should also form new coalitions to protect their common interests.

It is often claimed by e-commerce companies that they have worked hard towards developing a large local vendor base through various means including financial support, technology transfer, marketing support and skills development. Unfortunately, there is not enough data on the subject. This is an area which has not been adequately researched. In depth research would help in understanding the developmental contribution of e-commerce and will bring a balance to the debate that has seen criticism regarding huge gains of dominant players.

References

Ackerman, M. S., and Davis Jr, D. T. (2003). Privacy and Security Issues in E-commerce. New Economy Handbook, 911-930.

Adelola, T., Dawson, R., and Batmaz, F. (2015). Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches.

APEC. (2019). What is the Cross-Border Privacy Rules System? Asia-Pacific Economic Cooperation. 15 April. https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

Arun, S. (2017). Too Early To Regulate E-commerce: Jack Ma. The Hindu. 12 December.

ASG. (2019). Data Protection in India's Draft E-Commerce Policy: Key Takeaways for Businesses. Albright Stonebridge Group. 26 February. https://www.albrightstonebridge.com/files/ASG%20Analysis%20-%20Data%20Protection%20in%20India%27s%20Draft%20E-Commerce%20Policy_0.pdf

AU. (2019). List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection. 28 June. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

Avalara. (2019). Global VAT and GST On Digital Services. Avalara Inc. 2019. Accessed on June 10.

AVIA. (2019). Submission By The Asia Video Industry Association to the DPIIT On The Draft National E-Commerce Policy. Asia Video Industry Association. 29 March. https://asiavia.org/wp-content/uploads/2019/05/Final-Submission-to-DPIIT-on-the-Draft-National-e-Commerce-Policy.pdf

Banga, R. (2018). Is India Digitally Prepared for International Trade? RIS-DP # 235. Research and Information System for Developing Countries. November.

Banga, R. (2019). Modelling Impact of Moratorium on Electronic Transmissions using CGE: A Critique.

Baschuk, B. (2019). U.S. WTO E-Commerce Offer Reflects USMCA Digital Trade Chapter. Bloombergtax.com. May 6. https://news.bloombergtax.com/international-trade/u-s-wto-e-commerce-offer-reflects-usmca-digital-trade-chapter

Basu. A, Hickok. E, and Chawla. A.S. (2019). The Localisation Gambit - Unpacking Policy Measures for Sovereign Control of Data in India. The Centre for Internet and Society, India. 19 March.

Bauer, Matthias; Lee-Makiyama, Hosuk; Van der Marel, Erik; Verschelde, Bert (2014): The Costs of Data Localisation: Friendly Fire On Economic Recovery, ECIPE Occasional Paper, No. 3/2014, European Centre for International Political Economy (ECIPE), Brussels.

Beiten Burkhardt. (2018). China: Data Protection and Localisation, Cyber Security Law, VPN and Encryption. April.

Bird, R. (2018). Where Are We Now With Data Protection Law In China? Freshfields Bruckhaus Deringer LLP. Lexology. 13 September.

BIF. (2019). BIF Response To The 2019 Draft National E-commerce Policy. Broadband India Forum. https://www.broadbandindiaforum.com/images/Final%20BIF%20Response%20to%20Draft%20E-Comm%20Policy_%20V4_290319.pdf

BSA. (2017). Cross-border Data Flows. https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf

BSA. (2018). 2018 BSA Global Cloud Computing Scorecard. The Software Alliance. https://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

BSA. (2019). BSA Submission on Draft National E-Commerce Policy. The Software Alliance. 29 March. https://www.bsa.org/files/2019-03/03292019indiadraftecommercepolicy_0.pdf

CAIT web link on e-commerce. Confederation of All India Traders. http://www.cait.in/causes/fdi-in-e-commerce

Cate, F. H. (2006). The Failure of Fair Information Practice Principles. Consumer Protection in the Age of the Information Economy.

Cavoukian, A., and Castro, D. (2014). Big data and innovation, setting the record straight: de-identification does work. Information and Privacy Commissioner, 18.

CBPRS. (2019). Home page of the website. http://cbprs.org/

CCI. (2020a). Market study on E-commerce in India - Key Findings and Observations. Competition Commission of India. 8 January. https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf

CCI. (2020b). Order in the case between Delhi Vyapar Mahasangh (Informant) And Flipkart Internet Private Limited and its affiliated entities and

Amazon Seller Services Private Limited and its affiliated entities (Opposite Parties). Case No. 40 of 2019. Competition Commission of India. 13 January. https://www.cci.gov.in/sites/default/files/40-of-2019.pdf

Chakravorti. B, Bhalla. A, Chaturvedi, R. S. (2019). Which Countries Are Leading The Data Economy?. Harvard Business Review. 24 January.

Cheng, W., and Brandi, C. (2019). Governing Digital Trade - A New Role for the WTO (No. 6/2019). Briefing Paper.

Chun, S. H. (2019). E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability. Sustainability, 11(3), 715.

CIGI-Ipsos. (2019). 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. www.cigionline.org/internet-survey-2019.

CIS. (2019). CIS Response to Call for Stakeholder Comments: Draft E-Commerce Policy. The Centre for Internet and Society, India. 29 March. https://cis-india.org/internet-governance/resources/e-commerce-submission

Cory, N. (2017). Post-Hearing Written Submission. Before the United States International Trade Commission. Investigation No. 332-561. Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions. 21 April. http://www2.itif.org/2017-usitc-global-digital-trade.pdf

Cory. N, Atkinson. R.D., and Castro. D. (2019). Principles and Policies for "Data Free Flow With Trust". The Information Technology and Innovation Foundation (ITIF). 27 May.

Daimler. (2019). Privacy Statement. Data Protection Policy. https://www.daimler.com/privacy/

De Wachter, J. (2015). Is Data Really the New Oil? 1 September. http://jorendewachter.com/2015/09/is-data-really-the-new-oil/

Digital Empowerment Foundation. (2019). Submission of Comments on DIPP's Draft E-Commerce Policy. 29 March.

EC. (2016). EU-U.S. Privacy Shield. https://ec.europa.eu/info/sites/info/files/factsheet_eu-us_privacy_shield_en.pdf

ECIPE. (2018). DTE Report. Digital Trade Restrictiveness Index. European Center for International Political Economy. April.

ECIPE. (2019). The Economic Losses From Ending the WTO Moratorium on Electronic Transmissions. No 3/Policy Brief, ECIPE.

Ernst, D. (2016). The Information Technology Agreement, Manufacturing and Innovation – China's and India's Contrasting Experiences. East-West Center, Honolulu and Center for International Governance Innovation, Waterloo. 23 September.

Ertemel, A. V., & Civelek, M. E. (2018). The Effect of E-Commerce Web Site Security on Purchase Intention. Beykoz Akademi Dergisi, 6(2), 81-89.

EU. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council. 27 April. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1572868195313&uri=CELEX:32016R0679

Furnell, S. M., and Karweni, T. (1999). Security Implications of Electronic Commerce: a Survey of Consumers and Businesses. Internet Research, 9(5), 372-382.

G20. (2019a). G20 Finance Ministers and Central Bank Governors Meeting, Fukuoka, Japan. Communique. 8-9 June.

G20. (2019b). Osaka Declaration on Digital Economy. 28 June. https://g20.org/pdf/special_event/en/special_event_01.pdf and https://g20.org/en/special_event/

G20. (2019c). G20 Ministerial Statement on Trade and Digital Economy. 8-9 June.

García-Herrero, A., and Xu, J. (2018). How Big is China's Digital Economy?. Bruegel. 17 May.

Geist, M. (2018). The Sharing Economy and Trade Agreements: The Challenge to Domestic Regulation. In Tremblay-Huet S. (Author) & McKee D., Makela F., & Scassa T. (Eds.), Law and the "Sharing Economy": Regulating Online Market Platforms (pp. 223-260). University of Ottawa Press. Retrieved from http://www.jstor.org/stable/j.ctv5vdczv.11

Global Payments. (2018). Top 10 Fastest Growing Global E-Commerce Markets 2018. Edgar, Dunn & Company. Reproduced courtesy of PPRO.

Govt. of China. (2017). The 2nd Ministerial Meeting of Friends of E-Commerce for Development Held in Argentina. 12 December. http://english.mofcom.gov.cn/article/newsrelease/significantnews/201712/20171202688768.shtml

Govt. of France. (2019). France's Digital Tax Bill. 6 March. https://www.gouvernement.fr/sites/default/files/locale/piece-jointe/2019/04/11_taxe_gafa.pdf

Govt. of India. (2015). India and World Trade Organization (WTO) - Other Issues - Information Technology Agreement. Ministry of Commerce and Industry. https://commerce.gov.in/PageContent.aspx?Id=64

Govt. of India. (2017). Consolidated FDI Policy. Department of Industrial Policy and Promotion. Ministry of Commerce and Industry. https://

dipp.gov.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17.pdf

Govt. of India. (2019a). Transcript of Media Briefing by G20 Sherpa after G20 Summit 2019 in Osaka. Ministry of External Affairs. 30 June.

Govt. of India. (2019b). India's Trillion-dollar Digital Opportunity. Ministry of Electronics and Information Technology, Government of India. February.

Govt. of India. (2019c). Report on India's Trillion Dollar Digital Opportunity Released. Ministry of Electronics and Information Technology, Government of India. Press Release. Press Information Bureau. 20 February.

Govt of India. (2019d). Regulation of E-Commerce Companies. Ministry of Commerce & Industry. 4 December. https://pib.gov.in/Pressreleaseshare.aspx?PRID=1594910

Govt. of India. (2019e). Draft National e-Commerce Policy. February. Department for Promotion of Industry and Internal Trade. https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

Govt. of India. (2019f). Winter Session of Parliament Concludes. Ministry of Parliamentary Affairs. 13 December. https://pib.gov.in/PressReleseDetail.aspx?PRID=1596343

Govt. of India. (2019g). The Personal Data Protection (PDP) Bill, 2019. As Introduced In Lok Sabha. http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

Govt. of India. (2019h). Bill For Reference To Joint Committee. Lok Sabha. 11 December. http://loksabhadocs.nic.in/lobmk/17/Second/SLOB11.12.2019_.pdf

Govt. of India. (2019i). The Consumer Protection Act, 2019. Ministry of Law and Justice. The Gazette of India Extraordinary. 9 August. http://egazette.nic.in/WriteReadData/2019/210422.pdf

Govt. of India. (2019j). Goods and Service Tax (GST) - Concept and Status. Central Board of Indirect Taxes and Customs (CBIC). Department of Revenue. Ministry of Finance. Government of India. 1 April. https://cbic-gst.gov.in/pdf/01042019_GST-Concept-Status.pdf

Govt. of India. (2020). Budget 2020-2021 Speech of Nirmala Sitharaman Minister of Finance. 1 February. https://www.indiabudget.gov.in/doc/Budget_Speech.pdf

Govt. of Japan. (2019). Abenomics. https://www.japan.go.jp/abenomics/

Govt. of the US. (2000). Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress. Federal Trade Commission. May. https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

Govt. of US. (2019). Report on France's Digital Services Tax Prepared in the Investigation under Section 301 of the Trade Act of 1974. Office of the United States Trade Representative. 2 December. https://ustr.gov/sites/default/files/Report_On_France%27s_Digital_Services_Tax.pdfGSC. (2019). GSC Statement on The Indian Draft National e-Commerce Policy. Global Services Coalition. 8 March. https://www.keidanren.or.jp/en/policy/2019/023.pdf

Hamidi, H., and Moradi, S. (2017). Analysis of Consideration of Security Parameters by Vendors on Trust and Customer Satisfaction in E-commerce. Journal of Global Information Management (JGIM), 25(4), 32-45.

Herrero, A.G. and Xu, J. (2018). How Big Is China's Digital Economy?

Hongfei, Y. (2017). National Report On E-commerce Development In China. Inclusive and Sustainable Industrial Development Working Paper Series. WP 17/2017. United Nations Industrial Development Organization.

IBEF. (2019). E-commerce Industry in India. India Brand Equity Foundation. March.

Iberdrola. (2018). Iberdrola Personal Data Protection Policy. 18 December. https://www.iberdrola.com/wcorp/gc/prod/en_US/corporativos/docs/personal_data_protection_policy.pdf

IBM. (2017). Data Responsibility @ IBM. 10 October. https://www.ibm.com/blogs/policy/wp-content/uploads/2017/10/IBM_DataResponsibility-USLetter_WEB.pdf

ICC. (2019a). Taxation of Physical Goods in the Context of E-commerce: Avoiding Non-tariff Barriers through Simple and Consistent Design. WTO Plurilateral Negotiations on Trade-related Aspects of Electronic Commerce. International Chamber of Commerce. 11 September. https://iccwbo.org/content/uploads/sites/3/2019/09/icc-issues-brief-wc-e-commerce.pdf

ICC. (2019b). The Business Case for a Permanent Prohibition on Customs Duties on Electronic Transmissions. WTO Plurilateral Negotiations on Trade-related Aspects of Electronic Commerce. 11 September. https://iccwbo.org/content/uploads/sites/3/2019/09/icc-issues-brief-2-moratorium.pdf

Ido, V. (2019). Intellectual Property and Electronic Commerce: Proposals in the WTO and Policy Implications for Developing Countries. Policy Brief No. 62. South Centre. June. https://www.southcentre.int/wp-content/uploads/2019/06/PB62_Intellectual-Property-and-Electronic-Commerce-Proposals-in-the-WTO-and-Policy-Implications-for-Developing-Countries_EN.pdf

ING. (2017). 3D Printing: A Threat To Global Trade. September.

International Trade Centre. (2016). E-Commerce in China: Opportunities for Asian Firms. International Trade Centre, Geneva.

IPD Network. (2019). Website homepage http://www.redipd.es/index-ides-idphp.php

ITU. (2017). ICT Development Index 2017. IDI 2017 Rank. International Telecommunications Union.

Katie. (2019). Digital Taxes Around The World: What To Know About New Tax Rules. Quaderno. May 29.

Kumar, H.P. (2017). National Report On E-commerce Development in India. Inclusive and Sustainable Industrial Development Working Paper Series. WP 15/2017. United Nations Industrial Development Organization.

Leviathan Security Group. (2015). Quantifying the Cost of Forced Localization. June 24. https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf

López González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", OECD Trade Policy Papers, No. 205, OECD Publishing, Paris.

Mattoo, A and Meltzer, J. P. (2018). International Data Flows and Privacy - The Conflict and Its Resolution. Policy Research Working Paper 8431. World Bank Group. May.

Mandel, M. (2017). The Economic Impact of Data: Why Data is not like Oil. Progressive Policy Institute, Washington, DC, https://www. progressivepolicy. org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf.

Meghani, R. (2019). Top Six ECommerce Business Models In 2019 With Pros And Cons. Magneto IT Solutions. 14 March. https://magnetoitsolutions.com/blog/top-ecommerce-business-models

Miyazaki, A. D., and Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. Journal of Consumer affairs, 35(1), 27-44.

Monteiro, J. A., and Teh, R. (2017). Provisions On Electronic Commerce In Regional Trade Agreements. WTO Working Paper ERSD-2017-11. Economic Research and Statistics Division. World Trade Organization. July.

Myers, K. (2005). Petroleum, Poverty and Security. AFP BP 05/01.

Narayanan, A., and Felten, E. W. (2014). No silver bullet: De-identification still doesn't work. White Paper, 1-8.

NASSCOM. (2019). Comments on Draft National e-Commerce Policy. 29 March.

NTIA. (1999). Falling Through The Net: Defining The Digital Divide. A Report on the Telecommunications and Information Technology Gap in America. National Telecommunications and Information Administration. U.S. Department of Commerce. July.

OECD. (2001). Understanding The Digital Divide. Organisation for Economic Co-operation and Development.

OECD. (2019a). OECD Privacy Guidelines. http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

OECD. (2019b). Closing tax gaps - OECD launches Action Plan on Base Erosion and Profit Shifting. https://www.oecd.org/tax/closing-tax-gaps-oecd-launches-action-plan-on-base-erosion-and-profit-shifting.htm

OECD. (2019c). Addressing the Tax Challenges of the Digitalisation of the Economy – Policy Note. OECD/G20 Base Erosion and Profit Shifting Project. Organisation for Economic Co-operation and Development. 23 January.

OECD. (2019d). OECD Leading Multilateral Efforts to Address Tax Challenges from Digitalisation of the Economy. October 9. https://www.oecd.org/tax/oecd-leading-multilateral-efforts-to-address-tax-challenges-from-digitalisation-of-the-economy.htm

OECD. (2019e). OECD Secretariat Invites Public Input on the Global Anti-Base Erosion (GloBE) Proposal under Pillar Two. http://www.oecd.org/tax/oecd-secretariat-invites-public-input-on-the-global-anti-base-erosion-proposal-pillar-two.htm

O'hara, K., and Hall, W. (2018). Four Internets: The Geopolitics of Gigital Governance.

OWINFS. (2019). Statement from Civil Society Organizations Against E-commerce Rules in the World Trade Organization. Our World Is Not For Sale. 25 January. http://www.ourworldisnotforsale.net/2019/Digital_trade_WEF.pdf

Palit, A. (2019). India ducks Digital Trade Rules at G20. ISAS Brief. No. 65. Institute of South Asian Studies. National University of Singapore. 3 July.

Peck, S. W., and Chayes, S. (2015). The Oil Curse: A Remedial Role for the Oil Industry. Carnegie Endowment for International Peace.

Pinto, R. Á. (2018). Digital Sovereignty Or Digital Colonialism? Sur International Journal on Human Rights, July; 15(27), Page 15.

Ptashkina, M. (2018). Facilitation 2.0: E-Commerce And Trade In The Digital Age. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and Inter-American Development Bank (IDB). September.

Rapportrix. (2018). 6 Types of E-commerce Business Models. 22 June. https://www.rapportrix.com/6-types-of-e-commerce-business-models

Sarris, M. S. (2015). Consumer Trust Established by E-commerce Privacy Indicators (Doctoral dissertation, Capella University).

Schubert, S. R. (2006). Revisiting the oil curse: are oil rich nations really doomed to autocracy and inequality?.

Smith, S.R. (2017). Some Preliminary Implications of WTO Source Code Proposal. Third World Network Briefings. 10 December.

Stelly, R. (2019). Countries Table Proposals, Talks Continue On WTO E-Commerce Rules. Disruptive Competition Project. 23 August. http://www.project-disco.org/21st-century-trade/082319-countries-table-proposals-talks-continue-on-wto-e-commerce-rules/

Sugawara, J. (2019). Launch of "Osaka Track" on Digital Rules. Mizuho Economic Outlook and Analysis. Mizuho Research Institute Ltd. 2 July. https://www.mizuho-ri.co.jp/publication/research/pdf/eo/MEA190726.pdf

TrustArc Inc. (2019). TRUSTe Privacy Program Standards. https://www.trustarc.com/privacy-certification-standards/

Udo, G. J. (2001). Privacy and Security Concerns as Major Barriers for E-commerce: a Survey Study. Information Management & Computer Security, 9(4), 165-174.

UNCTAD. (2016). In Search of Cross-border E-commerce Trade Data. TECHNICAL NOTE NO 6 UNEDITED. TN/UNCTAD/ICT4D/06. United Nations Conference on Trade and Development. April.

UNCTAD. (2017a). Consumer Protection In Electronic Commerce - Note by the UNCTAD Secretariat. TD/B/C.I/CPLP/7. United Nations Conference on Trade and Development. 24 April.

UNCTAD. (2017b). E-Commerce for Development Ministerial by the Friends of E-Commerce for Development. United Nations Conference on Trade and Development. 25 April. https://unctad.org/en/Pages/MeetingDetails.aspx?meetingid=1360

UNCTAD. (2018). UNCTAD B2C E-commerce Index 2018. United Nations Conference on Trade and Development.

UNCTAD. (2019a). Global e-commerce sales surged to $29 trillion. United Nations Conference on Trade and Development. 29 March. https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2034

UNCTAD. (2019b). Growing Trade in Electronic Transmissions: Implications for the South. UNCTAD Research Paper No. 29. UNCTAD/SER.RP/2019/1. United Nations Conference on Trade and Development. February.

UNCTAD. (2019c). Summary of Adoption of E-Commerce Legislation Worldwide. United Nations Conference on Trade and Development. 27 March.

UNCTAD. (2019d). The Value And Role Of Data In Electronic Commerce And The Digital Economy And Its Implications For Inclusive Trade And Development. TD/B/EDE/3/2. United Nations Conference on Trade and Development. 23 January.

USISPF. (2019). USISPF Response To The Draft National E-commerce Policy, 2019. https://www.medianama.com/wp-content/uploads/USISPF-Final-Comments-Draft-National-eCommerce-Policy-v7-1.pdf

Van't Spijker, A. (2014). The new oil: using innovative business models to turn data into profit. Technics Publications.

Washington Trade Daily. (2019). Volume 28, Numbers 239, 240. 2 December.

Wes, M. (2017). Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization. International Association of Privacy Professionals (2017).

White, S. and Strupczewski, J. (2019). G20 Agrees To Wrap Up Big Tech Tax Rules By 2020. Reuters. 9 June.

Wong, W. P. M., Tan, K. L., & Lim, B. C. Y. (2019). The Effect of Technology Trust on Customer E-Loyalty in Online Shopping and The Mediating Effect of Trustworthiness. Wong, WPM, Tan, KL, Ida, AK, & Lim, BCY (2019). The Effect of Technology Trust on Customer E-Loyalty in Online Shopping and The Mediating Effect of

Trustworthiness. Journal of Marketing Advances and Practices, 1(2), 38-51.

World Bank. (2016). Digital Dividends. World Development Report 2016. The World Bank.

WTO. (1998). Declaration on Global Electronic Commerce. WT/MIN(98)/DEC/2. World Trade Organization. 25 May.

WTO. (1999). Work Programme On Electronic Commerce - Progress Report to the General Council. S/L/74. World Trade Organization. 27 July.

WTO. (2001). Dedicated Discussion on Electronic Commerce Under The Auspices Of The General Council On 15 June 2001 - Summary by the Secretariat of the Issues Raised. WT/GC/W/436. World Trade Organization. 6 July.

WTO. (2015). Briefing note: Information Technology Agreement. World Trade Organization. https://www.wto.org/english/thewto_e/minist_e/mc10_e/briefing_notes_e/brief_ita_e.htm

WTO. (2016a). Item 6 – Work Programme On Electronic Commerce - Review Of Progress - Report By The Chairman. WT/GC/W/728. World Trade Organization. 8 December.

WTO. (2016b). MIKTA Workshop on Electronic Commerce. 5 July. https://www.wto.org/english/news_e/spra_e/spra132_e.htm

WTO. (2017a). Joint Statement on E-commerce. World Trade Organization. 13 December.

WTO. (2017b). WTO, World Economic Forum and eWTP Launch Joint Public-private Dialogue To Open Up E-commerce For Small Business. World Trade Organization. 11 December.

WTO. (2017c). Work Programme On Electronic Commerce - Communication From Costa Rica. JOB/GC/139. World Trade Organization. 10 October.

WTO. (2017d). The Work Programme On Electronic Commerce. Statement By The African Group. JOB/GC/144. World Trade Organization. 20 October. (Also see JOB/GC/155 – 20 November, 2017).

WTO. (2017e). Work Programme On Electronic Commerce. Communication From China. JOB/GC/150. World Trade Organization. 10 November.

WTO. (2017f). Work Programme On Electronic Commerce. Communication From Australia, Canada, Chile, Colombia, the European Union, the Republic of Korea, Mexico, Montenegro, Norway, Paraguay, Peru and Ukraine. JOB/GC/140/Rev.3. World Trade Organization. 13 November.

WTO. (2017g). Work Programme On Electronic Commerce. Communication From India. WT/MIN(17)/27. World Trade Organization. 8 December. (Also see JOB/GC/13 - 17 November, 2017).

WTO. (2017h). Work Programme On Electronic Commerce. Communication From Bangladesh. WT/MIN(17)/29. World Trade Organization. 8 December. (Also see JOB/GC/152/Rev.1 - 19 November, 2017).

WTO. (2017i). Work Programme On Electronic Commerce. Communication From Bangladesh, Panama and Singapore. WT/MIN (17)/33. World Trade Organization. 9 December.

WTO. (2018a). Mainstreaming Trade To Attain The Sustainable Development Goals. World Trade Organization.

WTO. (2018b). Work Programme On Electronic Commerce Moratorium On Customs Duties On Electronic Transmissions: Need For A Re-think - Communication from India and South Africa. WT/GC/W/747. World Trade Organization. 13 July.

WTO. (2018c). Work Programme On Electronic Commerce - How Cyberspace "Intrudes" On The Physical Space? Case Studies: 3D Printing And The Sharing Economy. Non-Paper from the Separate Customs Territory of Taiwan, Penghu, Kinmen and Matsu. JOB/GC/171, JOB/CTG/13 JOB/SERV/278, JOB/IP/30 JOB/DEV/54. World Trade Organization . 15 February.

WTO. (2018d). World Trade Report 2018. The Future Of World Trade: How Digital Technologies Are Transforming Global Commerce. World Trade Organization.

WTO. (2018e). High-level Panel Highlights Potential Of E-commerce As Driver For Growth And Inclusion. World Trade Organization. 4 October. https://www.wto.org/english/news_e/news18_e/pf18_04oct18_e.htm

WTO. (2018f). WTO Negotiations On Trade-related Aspects Of E-commerce - Elements Of A Potential Approach Under The Framework Of The Joint Statement On Electronic Commerce: Communication from Argentina, Colombia and Costa Rica. JOB/GC/174. World Trade Organization. 5 April.

WTO. (2018g). Joint Statement On Electronic Commerce - Communication From New Zealand. JOB/GC/175. World Trade Organization. 11 April.

WTO. (2018h). Exploratory Work On Electronic Commerce - Non-paper From Brazil. JOB/GC/176. World Trade Organization. 11 April.

WTO. (2018i). Joint Statement On Electronic Commerce Initiative - Proposal For The Exploratory Work By Japan. JOB/GC/177. World Trade Organization. 12 April.

WTO. (2018j). Joint Statement On Electronic Commerce Initiative - Communication From The United States. JOB/GC/178. World Trade Organization. 12 April.

WTO. (2018k). Joint Statement On Electronic Commerce Initiative. Possible Elements For Exploratory Work On Electronic Commerce And Development. Communication from Singapore. JOB/GC/179. World Trade Organization. 13 April.

WTO. (2018l). Item 4 – Work Programme On Electronic Commerce – Review Of Progress. Report By Chairman. General Council. WT/GC/W/756. World Trade Organisation. 17 December.

WTO. (2019a). Annual Report 2019. World Trade Organization. https://www.wto.org/english/res_e/booksp_e/anrep19_e.pdf

WTO. (2019b). Work Programme on Electronic Commerce. The Economic Benefits of Cross-border Data Flows. Communication From the United States. S/C/W/382. World Trade Organization. 17 June.

WTO. (2019c). Joint Statement on Electronic Commerce. WT/L/1056. World Trade Organization. 25 January.

WTO. (2019d). Joint Statement On Electronic Commerce - EU Proposal For WTO Disciplines And Commitments Relating To Electronic Commerce. INF/ECOM/22. World Trade Organization. 26 April.

WTO. (2019e). Work Programme On Electronic Commerce - The E-commerce Moratorium And Implications For Developing Countries: Communication from India and South Africa. WT/GC/W/774. World Trade Organization. 4 June.

WTO. (2019f). WTO Members Agree to Extend E-commerce, Non-violation Moratoriums. World Trade Organisation. 10 December. https://www.wto.org/english/news_e/news19_e/gc_10dec19_e.htm

WTO. (2019g). Joint Statement On Electronic Commerce. Communication from China. INF/ECOM/19. 24 April.

WTO. (2019h). Joint Statement On Electronic Commerce. Communication From Brazil. Revision. INF/ECOM/27/Rev.1. 9 July.

WTO. (2019i). Joint Statement On Electronic Commerce. Communication From The United States. INF/ECOM/23. 26 April.

WTO. (2019j). Joint Statement On Electronic Commerce. Communication from Singapore. INF/ECOM/25. 30 April.

WTOa. MC11 In Brief. Electronic Commerce. World Trade Organization. https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm

WTOb. WTO Analytical Index GATS – Article XIV (Practice). https://www.wto.org/english/res_e/publications_e/ai17_e/gats_art14_oth.pdf

WTOc. General Agreement on Trade in Services. World Trade Organization. https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleIX

WTOd. Information Technology Agreement - An Explanation. World Trade Organization. https://www.wto.org/english/tratop_e/inftec_e/itaintro_e.htm

WTOe. Electronic Commerce. World Trade Organization. https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

WTOf. Trade Facilitation. https://www.wto.org/english/tratop_e/tradfa_e/tradfa_e.htm

Wu, Mark. (2017). Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB). November.

Zhang, L and Chen, S. (2019). China's Digital Economy: Opportunities and Risks. IMF Working Paper. WP/19/16. International Monetary Fund. January.

About the Report: In an era where the digital economy is being globalised at a fast pace, governments and policy makers across the world are trying to address the sensitivities involving cross-border data flows as well as the ramifications of a few developed nations and big firms dominating the e-commerce sector. This Report attempts to give an overview of the developments related to e-commerce rule-making at the multilateral / plurilateral discussions under the auspices of the World Trade Organization, at the bilateral and regional platforms (i.e., lessons from the Regional Trade Agreements) as well as at the national level – namely in India, which is among the world's fastest growing e-commerce markets. On the basis of a review of literature and stakeholder discussions, the Report advocates a balanced approach in such rule-making - at all the above-mentioned levels - that ensures sufficient policy space to countries to safeguard their vital national security objectives, protect the fundamental rights of their citizens, and meet their developmental needs, while eliminating barriers to enable sustainable national and cross-border e-commerce.

About RIS: Research and Information System for Developing Countries (RIS) is a New Delhi-based autonomous policy research institute that specialises in issues related to international economic development, trade, investment and technology. RIS is envisioned as a forum for fostering effective policy dialogue and capacity-building among developing countries on global and regional economic issues.

The focus of the work programme of RIS is to promote South-South Cooperation and collaborate with developing countries in multilateral negotiations in various forums. RIS is engaged across inter-governmental processes of several regional economic cooperation initiatives. Through its intensive network of think tanks, RIS seeks to strengthen policy coherence on international economic issues and the development partnership canvas. For more information about RIS and its work programme, please visit its website.

RIS
Research and Information System for Developing Countries
विकासशील देशों की अनुसंधान एवं सूचना प्रणाली

Core IV-B, Fourth Floor, India Habitat Centre
Lodhi Road, New Delhi-110 003 India., Ph. 91-11-24682177-80
Fax: 91-11-24682173-74, Email: dgoffice@ris.org.in
Website: www.ris.org.in

Follow us on:

www.facebook.com/risindia @RIS_NewDelhi www.youtube.com/RISNewDelhi