

CIS Response to Call for Stakeholder Comments: Draft E-Commerce Policy

March 29, 2019

By (in alphabetical order) **Amber Sinha, Arindrajit Basu, Elonnai Hickok & Vipul Kharbanda**

The Centre for Internet and Society, India

Preliminary

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on the internet and digital technologies from policy and academic perspectives. Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and practices around the internet, technology and society in India, and elsewhere.

CIS is grateful for the opportunity to submit to the Department of Industrial Policy and Promotion comments to the draft National e-commerce policy. Over the last decade, CIS has worked extensively on research around privacy, cross border flows of data, security, and innovation.

Introduction

The E-Commerce Policy is a much needed and timely document that seeks to enable the growth of India's digital ecosystem. Crucially, it backs up India's stance at the WTO, which has been a robust pushback against digital trade policies that would benefit the developed world at the cost of emerging economies. However, in order to ensure that the benefits of the digital economy are truly shared, focus must not only be on the sellers but also on the consumers, which automatically brings in individual rights into the question. No right is absolute but there needs to be a fair trade-off between the mercantilist aspirations of a burgeoning digital economy and the civil and political rights of the individuals who are spurring the economy on. We also appreciate the recognition that the regulation of e-commerce must be an inter-disciplinary effort and the assertion of the roles of various other departments and ministries. However, we also caution against over-reach and encroaching into policy domains that fall within the mandate of existing laws.

In this submission, we seek to provide some high-level comments on broader issues on the policy and the ecosystem and then go into section by section commentary. Some comments recommend a change in the policy framework while others provide supplementary information that could be used to justify existing stances or be useful at the enforcement stage. Our comments are limited to Parts I to IV of the e-commerce policy and do not extend to Parts V and VI.

High-Level Comments

- **Objective and structure:** The policy currently reads as both a vision document and foundational framework for the emergence of laws and policies in the future. It accurately identifies the main challenges for the digital economy:
 - (1) Market concentration in the hands of a few, largely foreign players
 - (2) Storage of data abroad can complicate access for local innovation as well as impact rights.
 - (3) Potential for abuse of data and individual rights by the private sector
 - (4) Incorporating the rights of vulnerable communities.
 - (5) Ensuring security of the digital economy and consequences for a nation.

Even though the policy identifies these challenges in the ‘Vision Section,’ the operative components of the policy appear to focus on the economy as a whole, rather than the individuals who are meant to benefit from it. It might be tempting to believe that a burgeoning economy would boost prosperity for individuals but it is important to also ensure that this prosperity does not result in a Faustian bargain where the consumer is compelled to trade away civil rights or is disparate in the sense that it privileges certain sections of the society over others.

Further, the objective of the policy is unclear: In parts, it operates as a guiding vision document that identifies core principles and provides broad recommendations to government departments to develop workable frameworks. In other parts, it draws up specific requirements, such as the requirement on restricting cross-border data transfer.. In the absence of an explicit declaration that charts out the operational objective of the policy, businesses-both Indian and foreign-and consumers will be faced with great uncertainty and not be aware of how to use the policy to frame business or consumption decisions.

- **Definitions:** The Annex contains several definitions of ‘e-commerce.’ One definition that can be used throughout the policy is necessary to foster certainty and stability in the ecosystem. Further, various other terms like ‘sensitive data,’ ‘consent’ ,’network effect’ that appear throughout the document have not been clearly defined. Several of these terms have been defined in existing laws or draft Bills and the finalised policy needs to state clearly if the definitions are *in pari materia* with existing laws and policies.

- **Placing policy in the context of other developments:** This policy is being introduced in a context where a number of policies seeking to regulate India's digital ecosystem. These include the Draft Data Protection Bill, Draft Information Technology [Intermediary Guidelines (Amendment)] Rules, 2018 along with various policy moves at the World Trade Organisation. Several themes-such as cross border data flows, data protection and obligations of both foreign and Indian private sector players come up across all policies. It is important to note that each policy performs a key role in fostering innovation while protecting rights. It is equally important to ensure that there is an element of cohesion across all policies. The e-commerce policy appears to be mindful of this but surprisingly, ventures into avenues that do not fall within its domain.,

- **Components that do not belong in the policy**

While the following are key aspects for the policy to be cognizant of, they need to be aligned to existing or emerging frameworks that speak exclusively to these policy areas:

 - Data protection (covered by draft Data Protection Bill, 2018)
 - Intermediary Liability (Covered by Section 79A IT Act and any the draft of the Information Technology [Intermediary Guidelines (Amendment) Rules 2018]
 - Anti-piracy (Indian Copyright Act,1957 While this regime is not comprehensive and clearer rules need to be framed, anti-piracy belongs in the domain of IP law and enforcement, not in an e-commerce policy that is focussing on the digital economy and strategies for fostering inclusive growth.)
 - Data localization: *Considering the complexities of the issue and the variety of stakeholders involved, an E-commerce policy is not the correct instrument to push a data localization mandate across sectors, as this policy documents seems to be suggesting.*

Specific Provisions

Guiding Principles and Approach

The e-commerce policy highlights the importance of a regulatory framework for privacy, consumer protection, and the flow of data that benefits India's domestic economy by ensuring market competition. We would urge the DPIIT to commission research to inform the decisions in the policy to ensure that such decisions are backed by evidence based

research of both positive and negative impacts across stakeholder groups and sectors. While we welcome the importance placed on creating a framework that benefits India's domestic economy and the inclusion of privacy and e-commerce - we believe that these guiding principles could be strengthened through the additional principles and approach.

1. **Rights Driven Approach:** Complimenting a market driven principles to the policy, we would entreat the DPIIT to place the protection of individual rights as core principles guiding the policy. This will include recognizing the importance of comprehensive frameworks and practices for privacy and data protection and freedom of expression as well as policies that enable fair access to digital services as key precursors to enabling companies participating in e-commerce to undertake practices that respect, uphold, and enable individual rights.
2. **Security:** The guiding principles would benefit from including a recognition and emphasis on cyber security and fully complying with existing cyber security frameworks and requirements in India as a guiding principle towards enabling a secure and trusted e-commerce environment that benefits India's domestic economy.
3. **International Relations:** India has taken a leadership role, along with other emerging economies such as South Africa to keep e-commerce outside tariff reduction negotiations at the WTO.¹In particular, the policy identifies correctly that India has opposed the moratorium on imposing customs duties on electronic transmissions. India intervened at this debate on 27th November 2018 along with South Africa.² While this front is needed for emerging economies, India should be careful to ensure that recommendations in this policy-particularly on data localisation do not become a thorn in bilateral trade ties with EU and US. Therefore, there should be continuous coordination between the DPIIT and the Department of Commerce to ensure that India's objectives are explained in a positive light to global partners.

Scope and Objectives

The objective of the e-commerce is the construction of a robust ecosystem for the burgeoning of indigenous e-commerce platforms in india. To do so, it stresses multiple times on the economic value of data. The policy should build adequate safeguards in

¹[https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785,](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785)

²[https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785,](https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=247027,247023,246849,246824,246785)

place to ensure that the *fruits of this economic value enables rights and economic empowerment for individuals rather than being restricted to large corporations.*

However, the extraction of economic value from data is conditional on the ability of all players in the market to annotate and process the data sets. The policy appears to first focus on access to data following which concerns revolving around the utility of these datasets will be taken into account. Instead, to achieve the overarching objective or a robust ecosystem for e-commerce, both these processes need to be undertaken simultaneously. The government needs to start thinking about how smaller players can be incentivised and subsidised such that they have the requisite infrastructure, technological capacity and skills to process the data adequately.³

I. Data

Conceptualization of Data

While we appreciate the DPIIT's recognition that data is a valuable resource for individuals, corporations, and decision makers and India as a nation - we would recommend the following:

1. **Technical orientation:** The policy notes that data generated over the internet is automatically stored in the data cloud. This is not necessarily the case and depends on the architecture of each service, platform, and service provider. Having the correct technical orientation is important as it is key in informing policy decisions around enabling access to data by different actors - individuals, private sector, public sector, and law enforcement.
2. **Nuanced conceptualization of data:** The policy currently approaches data broadly without making distinctions between non-identifying data, personal data and sensitive personal data as well as the different purposes for which the data may accessed and used for. In doing so the policy does not recognize the fact that

³ "On the other hand, Israel is a model for start-up incubation that has thrived without any sort of data localisation. Israel has 7,000 start-ups, 350 VC funds and over 300 corporate R&D centres. Israel does not have any policy that restricts the cross-border flow of data in place. However, just as in the case of China, the thriving tech sector in Israel may owe more to factors other than a mere lack of restriction on cross border flow of data. As argued by Senon and Singer, the growth in the tech sector in Israel has hinged around : (1)Education and Research: The government spends 4.3% of its GDP on Research & Development while India spends just 0.8%. (2)Immigration: Senon and Singer believe that the work ethic and risk-taking drive in migrants has further propelled the start-up economy. and (3) Government support and enabling ecosystem: The Israeli Government plays a vital role in the startup and innovation ecosystem, both directly and indirectly. Directly, it supports 19 entrepreneurship programs, funds, and incubators" See Basu A, Hickok E and Chawla A, " The Localisation Gambit: Unpacking policy moves for sovereign control of data in India <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>

when in combination with other data points, non-identifying data can become personal or sensitive personal.

3. **Emphasis on data quality:** While the policy recognizes the importance of large quantities of data, it does not place an equal emphasis on the quality of data. Ideally, the quality and quantity of data are given equal importance as is curation of the data. Without adequate emphasis on data quality there is a risk that analysis is incorrect or biased. Standards for data collection, cleaning, curation, and storage are important in ensuring data quality.⁴
4. **Individual data ownership:** The policy takes the position that the individual owns his/her data. Thus, if data of an individual is used - it must be with express consent. Though consent is an important factor in ensuring that an individual has control over his/her data - research has 1. Demonstrated that consent fatigue is weakening the strength of consent as many people consent without fully understand what they are consenting to 2. Found that other data rights including - access, portability, right to be informed, right to rectification, right to object etc. - are important in ensuring that the individual has control over his/her data. We would recommend that individual data ownership be conceptualized from a clear set of individual data rights and data controller responsibilities as opposed to hinging only on consent.
5. **Data as a collective property of the group and national resource:** The policy notes that data of a group is the collective property of the group - that data generated in India belongs to Indians and is a national asset that the governments holds in trust but which rights can be permitted. We would recommend that as the government begins to establish frameworks to further leverage data - each framework is grounded in privacy as a fundamental human right. From this right to privacy - a set of data rights are necessary to enable and empower the individual in today's data driven society. The government has the responsibility of protecting this right including ensuring that both the private sector and public sector do not undertake exploitative practices and that robust mechanisms of accountability and oversight are in place for the same. Overlooking privacy as a fundamental right and the needed framework to enable this and treating data purely as a national resource can inadvertently enable an exploitative culture that undermines individual dignity and autonomy and replicated existing practices that can be seen globally. .
6. **Enabling equal access “Essential Facilities Doctrine”:** The policy puts forth that as a national resource, data should be equitably accessed by all Indians. Though it is important to create a level playing field - we would urge the DPIIT to create a

⁴Basu A and Hickok E “ Artificial Intelligence in the Governance Sector in India”
<https://cis-india.org/internet-governance/ai-and-governance-case-study-pdf>

more robust framework on how this access would be facilitated and protect against larger Indian companies dominating access to data. Furthermore, we would recommend the framework place obligations on private sector companies to be the main actor opening up their data for use. A proportionate approach could be taken with larger companies needing to open up larger amounts of data. There also needs to be in place robust mechanisms to monitor and track how data is being used.

A useful framework to legitimize access to data might be the ‘essential facilities doctrine’ which has evolved in comparative competition law and is currently being seeded in Indian competition law doctrine as well. Essentially, this doctrine imposes obligations on a natural monopolist to share its “essential facilities: with every player asking for access including competitors both in the market where there is a natural monopoly and other downstream markets that access to the facility may impact. This doctrine operates as an exception to the tenet of anti-trust and competition law, which allows all players including monopolists to strike a deal with other players of the choosing⁵ and has come under some criticism for not being economically or legally viable.⁶

This doctrine has been examined by the Competition Commission of India (CCI) in *Arshiya Rail Infrastructure Limited (ARIL)*⁷. The CCI decided that the monopolist in question was not dominant in the market but as *obiter dictum*, mentioned that the essential facilities doctrine could be invoked if the following conditions are met :

1. Technical feasibility of providing access on reasonable terms;
2. Feasibility of replicating the facility in a reasonable period of time, distinct possibility of lack of effective competition if such access is denied and possibility of providing access on reasonable terms..

The landmark judgement of *Shamsher Kataria v. Honda Siel Cars India Ltd*⁸, took this forward and concluded that spare parts, diagnostic tools and manuals would constitute essential facilities for repairers to effectively provide the service to the

⁵ Gundlach, Gregory T., and Paul N. Bloom. “The ‘Essential Facility’ Doctrine: Legal Limits and Antitrust Considerations.” *Journal of Public Policy & Marketing*, vol. 12, no. 2, 1993, pp. 156–169

⁶ David Reiffen & Andrew N. Kleit, *Terminal Railroad Revisited: Foreclosure of an Essential Facility or Simple Horizontal Monopoly?*, 33 *Journal of Law&Economics*. 419, 420–21 (1990); Herbert J. Hovenkamp, *Unilateral Refusals to Deal, Vertical Integration, and the Essential Facility Doctrine* 4 (Univ. of Iowa Legal Studies, Research Paper No. 08-31, 2008), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1144675.

⁷ <https://www.cci.gov.in/sites/default/files/642010T.pdf>

⁸ <https://www.cci.gov.in/sites/default/files/03201127.pdf>

consumers. The parameters needed to decide whether a factor of production would count as an essential facility were delineated as follows:

- (a) control of the essential facility by the monopolist;
- (b) the inability to duplicate the facility;
- (c) the denial of the use of the facility; and
- (d) the feasibility of providing the facility.

While there is no legal pronouncement extending this doctrine to online platforms, some secondary literature has investigated the prospects of characterising big data as an essential facility and therefore imposing a duty of non-discriminatory access to the data in question.⁹ Kubcik argues that, for this purpose, it might be incorrect to characterise all data as an essential ‘facility’ in a market and granularly segregate data that meets the characteristics enlisted in the four-pronged test.¹⁰ Khan, in her oft-cited law review article ‘Amazon’s Anti-Trust Paradox goes so far as to say that Amazon should provide access to all its infrastructure.’¹¹

7. **Emphasis on security:** The policy is broadly silent on the importance of security and how e-commerce services will be required to comply with existing security frameworks and standards. As India continues to develop digital infrastructure for the nation - cyber security is key in ensuring trust and reliability of services. The policy would benefit from articulating how it will align with and encourage improvement of existing security frameworks. India needs to simultaneously improve its cyber security posture and continue to build capacity in public sector officials and bodies.
8. **Beyond Anonymization:** Though the policy notes that data should be anonymized. It is not clear that this is a sufficient safeguard. A number of studies have shown that due to the relatively few parameters required to trace back to an individual, anonymization is often not a strong enough system to guarantee privacy and security¹²
9. **Indian Sources of Data:** The policy notes that Aadhaar, BHIM, and eKYC are Indian sources of data that can be leveraged for innovation. Towards ensuring that India leverages the data of its citizens and residents it will be critical that the government ensures that public sector data can be accessed and used without hindrance by the public sector by the government. The next step will be to open up this data for use by the public.

⁹ Jan Kupcik (2018), “ Why real big data might not matter that much and why data portability is crucial”
http://ec.europa.eu/competition/information/digitisation_2018/contributions/jan_kupcik.pdf

¹⁰ Ibid

¹¹ Lina M Khan, “Amazon’s Anti-trust paradox” Yale LJ (2017)

¹² Schneier B, “Why anonymous data sometimes isn’t”

<https://www.wired.com/2007/12/why-anonymous-data-sometimes-isnt/>

10. **Data rights:** The policy underscores the important role that the RTI Act has played in empowering individuals. Just as the RTI has given individuals the right to request information from the public sector, individuals need to be empowered with robust set of data rights. The one's articulated in the draft Data Protection Bill 2018 area good starting place.
11. **Open data:** The policy currently does not reference open data. Building upon the existing open data framework that exists in India is a positive way to enable Indians to leverage India's data towards further innovation and development.¹³

Proposed Restrictions on Cross-Border Flow of Data

Section 1.1

The restrictions on cross-border flow of data envisaged by the policy is an addition to a litany of laws and regulations that are stressing on the need to ensure access of Indian companies to data so that it may be used for India's development. In a recently published working paper on Data Localisation, CIS delved deeper into some of these assumptions.

Andrew Ng has argued that the benefits of big data may be overstated,¹⁴ since beyond the availability of data, demarcating, picking and operationalizing enough **relevant** data sets is still a challenge.¹⁵ Insiders at Tencent have claimed that the company finds it difficult to integrate various data streams due to various logistic and technical hurdles.¹⁶ **It is crucial to remember that the mere availability of vast quantities of data does not enable AI development. The quality of data, which is a function of research, infrastructure and other factors outlined above are equally important for harnessing that data - for which data localisation is an inadequate stand alone solution.**

Further, the policy needs to take into consideration the challenges inherent in generating revenue from data collected. An IBM report estimates that 80% of all available data is

¹³ Isha Parihar (2015), "How is open data changing India?"
<https://www.weforum.org/agenda/2015/02/how-is-open-data-changing-india/>

¹⁴ S. LeVine, Axios Future Newsletter, October 18 2018,
<https://www.axios.com/newsletters/axios-future-5443c000-9035-4915-8924-6158c6a37bf7.html?chunk=0&utm_term=emshare#story0>

¹⁵ D. Pereira, Andrew NG's "The State of Artificial Intelligence" reviewed, January 9 2018,
<<https://medium.com/@dpereirapaz/andrew-ngs-the-state-of-artificial-intelligence-reviewed-7007d95a72a1>>

¹⁶ R. Zwetsloot, H. Toner, and J. Ding, Beyond the AI Arms Race, November 16 2018,
<<https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race>>

unstructured and therefore 'dark'¹⁷ Given challenges to adequately labelling and processing datasets in a manner that generates economic utility and enables easy use for further innovation, we believe that it is important that the e-commerce policy account for several prerequisite questions to ensure that access to data is not the only prerequisite objective to enabling innovation: :

- ★ Sustainability of energy consumption and the cost of other basic utilities
- ★ Wireless Bandwidth
- ★ Favourable tax regime that enables growth of data centres
- ★ Downstream infrastructure such as uninterrupted power supplies, including roads and electrical connectivity
- ★ Significant expenditure on cooling due to unfavourable weather patterns. An adequate costing of this is required to understand the impact of weather patterns on setting up of data centres.
- ★ Robust security safeguards which would include both **physical and logistical protection** for the data centres (including but not limited to access filters such as biometric authentication, for data centres containing sensitive personal information-armed personnel from law enforcement authority or a recognized private security company and strong physical fortifications), rigorous checks on the infrastructure to ensure it complies with infrastructural requirements to guarantee maximum safety and security and **technical measures** including but not limited to protection against unauthorized remote access to the data centre, maintenance of a back-up in another physical location.
- ★ The extent to which smaller players have the financial and technical capacity to gain from access to data as much as the larger players. In the absence of the government financially subsidizing and also aiding their technical capacity, it is likely that the benefits of localisation will be reaped only by the larger Indian private corporations, and potentially some Chinese ones like AliBaba and Xilinx that already have data centres here.¹⁸ In a study of fifty-one stakeholders who had commented on data localisation in India, we found that two constituencies in favour of the move were large

¹⁷ Kristifoe, "Marketing in the dark-Dark Data", 2018, <https://www.ibm.com/blogs/think/be-en/2018/04/24/marketing-dark-dark-data/>

¹⁸ It is important to note that the Chinese companies did not support the localisation mandate because it would entail automatic access to data but because it would lead to a competitive disadvantage for other foreign market rivals who do not have data centres in India

Indian corporations like Reliance and Phone Pe and large Chinese corporations like AliBaba and Xilinx, which explains the potential dividend that they can reap from this move, potentially at the cost of smaller players. It is the prerogative of the government to ensure that the benefit is equitable.

Section 1.2

Section 1.2 of the Policy is responsible in that it places conditional obligations on business entities that collect or process sensitive data. The only potential problem is the erosion of interoperability through consumer consent. Apart from that, if a conditional approach is also extended to all types of data, the objectives of data localisation-which lie in ensuring greater access to and security and privacy of data by Indian entities, can be achieved without having to bear the economic, political or diplomatic costs.

However, a core operational issue with the clause is that it does not discuss the conflict of laws problem that any business entity may have to grapple with. Another issue is that this policy has not devised a framework that regulates the process by which a government or non government entity can request for data stored abroad in order to fulfil the objectives listed out in this policy. Additionally, the provision is silent on how this would align with existing provisions around access in India. Therefore, it should also seek to place obligations on any state to which Indian citizens' data is being transported to. Second, it does not enable data portability to a third party even if the consumer consents, which reduces the significance of consent in the data protection framework. As stated before, it is imperative that India brings about a robust, enforceable data protection framework that guarantees the civil liberties of all Indian citizens and residents. Thus we recommend re-wording Section 1.4 to

“ Any state to which hosts business entities that collects or processes any data in India must:

1. Place obligations on business entities which ensure that
 - (a) All such data stored abroad shall not be made available to other business entities outside India,
 - (b) All such data shall not be made available to a third party for any purpose
 - (c) All such data stored abroad shall not be made available to a foreign government for any purpose

NB: Exception: If the data in question is 'public data,' then the nodal agency can approve an exception to (a), (b) and (c). If it is personal data, then the consent of the individual must be sought.

2. Any legal request from Indian authorities to have access to data concerning Indian citizens or residents stored in the territory of said country must be complied with based on Indian law. A Responsible Nodal officer (possibly the Data Protection Authority set up under the Personal Data Protection Bill under section 41) could be appointed for ensuring the smooth transfer of data and compliance with the defined conditions in the policy and the data protection legislation. Failure to comply with these requirements will result in Indian authorities not allowing the cross-border transfer of data into said territory.
3. Develop a legal data protection and human rights framework with safeguards that are equivalent to those in India

Section 1.4 - Community Data

When defining community data, the SriKrishna Report endorses a collective protection of privacy by protecting an identifiable community that has contributed to community data. The according of this protection requires the fulfilment of three key aspects :

- (1) The data belongs to an identifiable community and
- (2) The individuals in the community consent to being a part of the community and
- (3) the community as a whole consents to their data being treated as community data.

The focus in the SriKrishna Bill and indeed, in the examples of the identifiable indigenous communities in New Zealand and Canada provided in the Annex of the Policy, is the protection of community data. The e-commerce policy instead appropriates the notion of community data and re-conceptualizes it instead as 'societal commons' or a 'national resource.' It is crucial that personal data is only treated as 'community data' if the three-pronged requirements are satisfied, failing which the operative sections of the policy would be violating the consent framework in the Sri Krishna Bill and in various other comparative law instruments across the world.

II. Infrastructure

A robust digital economy that aids the country's development trajectory requires a physical infrastructure as well. This section delineates broad strategies to achieve this.

The changes that the policy proposes to data management and consequently to infrastructure development will have implications beyond the e-commerce sector.

Strategies

2.1 'Digital India' consists of three core components: (i) the development of secure and stable digital infrastructure; (ii) delivering government services digitally; and (iii) universal digital literacy. This Policy aims to take forward these core components to realise the objectives envisaged in this document.

2.2 Steps will be taken to develop capacity for data storage in India. An assessment needs to be done regarding how data-storage-ready the available infrastructure in the country is. Creation of infrastructure for storage would take some time. 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. Certainty about the intent and direction of government policy is important to maximize private investment in this sector.

Comment: *The effect that such a move towards localization would have on the tech industry as a whole is also only cursorily considered with the industry being given a time period of three years to adjust to the new requirements. The policy does not provide evidence as to whether such an adjustment period is adequate or not. Further, an adjustment period is not a standalone solution to the various challenges that local technology companies may face due to such a move. Importantly, the policy is silent on issues such as cost, service standards, etc.*

2.3 The Harmonized Master List of Infrastructure -sectors grants 'infrastructure status' to certain categories of sectors, goods and services to guide the various agencies responsible for supporting infrastructure in various ways, including financing their development. This enables regulation of the listed infrastructure in a more streamlined manner. Benefits of such regulation have led to India having one of the largest roadways and railway networks in the world. Data centres, server farms, towers and tower stations, equipment, optical wires, signal transceivers, antennae etc. will be accorded 'infrastructure status' Physical infrastructure for setting up of data centers (power supply, connectivity etc.) will be established by the relevant implementing agencies, while financing agencies may identify these as infrastructure that they may intend to support. This would facilitate achieving last mile connectivity across urban and rural India, including hilly areas, as aimed under the Digital India initiative.

Comment: *While inclusion of digital infrastructure in the Harmonized List is a welcome measure, this by itself may not be enough to develop a competitive digital infrastructure marketplace in India. A wider process involving deeper consultation with stakeholders and potential entrepreneurs is needed to understand all the issues that may need to be addressed in order to develop a robust and competitive digital infrastructure in India.*

2.4 Domestic alternatives to foreign-based clouds and email facilities will be promoted. Ways of promoting this could include budgetary support.

Comment: *It is not clear why budgetary support is envisaged only for domestic Cloud and email services and not for other digital infrastructure such as ISPs, server farms, etc. as well.*

III. E-commerce marketplace

- There is ambiguity introduced by the difference in the definition of e-commerce in the Policy and Press Note 2 of 2018 issued by the erstwhile Department of Industrial Policy and Promotion that regulated foreign direct investments (“FDI”) in the e-commerce sector. While Press Note 2 defines e-commerce to mean “buying and selling” of goods and services, the Policy defines e-commerce as including “buying, selling, marketing or distribution” of goods and services. The definition in the Policy is much more expansive and applies to not just the acts of buying and selling to all other aspects of the ecommerce trade. The variance in the two definitions is bound to cause confusion in the future for companies who may fall in the corner cases. A clarification on this would be helpful in the future. It is recommended that the definition of e-commerce is aligned in both the drafts.
- The Policy pays a significant amount of attention to the regulatory framework surrounding the import of goods into India. It is noted that the Policy recommends very severe regulations such as requiring all e-commerce sites/apps available for download in India to have a registered business entity in India and be the importer on record or the entity through which all sales in India are transacted, without exploring all the potential roadblocks in effective implementation of such regulation. Further, regulatory suggestions such as “any payments to GST non-compliant sites/ apps through Indian banks and payment gateways to be barred” show a lack of appreciation of the existing operational challenges with the GST regimes, and are inappropriate policy responses. Other recommendations requiring India Post to conduct due diligence on shipping entities and addresses and set thresholds to eliminate misuse of the “gift” route, also does not take into account the capacity challenges of such a move.
- There are also several anti-counterfeit measures in the Policy. It states that e-commerce platforms must provide an option to trademark owners (including licensees) to register themselves on the e-commerce platform (“Platform Registered TM Owners”), and whenever a trademarked product is uploaded for sale on the e-commerce platform, such ecommerce platforms shall notify such Platform Registered TM Owners. This puts severe operational costs on the platform to address an issue that better addressed through better implementation of trademark law.

IV. Regulatory Issues

B Data Lens

4.6 Advertising and data collection

The policy validly addresses the problem of exorbitant advertisement fees charged by social media platforms . An equally important question is the erosion of free and informed consent on the part of the consumer when faced with what is effectively a monopoly. Germany's Federal Cartel Office, the country's antitrust regulator has recently held that Facebook was exploiting consumers by compelling them to agree with the terms of data collection in order to operate an account.¹⁹ The FCO also argued that Facebook used its vast data collection to build up its market dominance, therefore squeezing meaningful choice away from the consumers. While this point validly considers the plight of the smaller players and therefore mandates the restriction of charges, it should also look into the role of meaningful consent in the digital economy as this not only has implications for individual rights but also for a free and fair, competitive market.

4.7 and 4.8 Market Distortions

The market distortions mentioned in 4.7 and 4.8 are crucial and are rightly tackled in this policy. However, the distortions exist due to a fundamental reorientation of anti-trust and competition law worldwide in the recent decade, which allows distortions like this to thrive. While the policy is a good place to start, an overarching rehaul of competition law in India is also the need of the hour.

As Khan documents²⁰, there was a shift in the global approach to anti-trust with the rising prominence of the Chicago School in the 1970s which were driven by the fundamental assumption (as argued by one of their champions) "[R]ational economic actors working within the confines of the market seek to maximize profits by combining inputs in the most efficient manner. A failure to act in this fashion will be punished by the competitive forces of the market." ²¹Before the emergence of the Chicago School, anti-trust was governed by structuralism which was founded on the idea that concentrated market structures are inherently anti-competitive. This is due to four reasons :(1) Concentrated structures enable dominant actors to coordinate with greater ease, thereby facilitating anti-competitive practices like price-fixing, market division and tacit collusion, (2) Abuse

¹⁹ "Bundeskartellamt prohibits Facebook from combining user data from various sources"https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html

²⁰ Lina M Khan, "Amazon's Anti-trust paradox" Yale LJ (2017)

²¹ Marc Allen Eisner, Antitrust and the Triumph of Economics: Institutions, Expertise, and Policy Change 107 (1991).

of dominance to block new entrants, (3) Greater bargaining power for monopolistic firms against consumers, suppliers and workers.²²

Khan goes on to argue that the Chicago anti-trust framework that pegs competition to a reductionist understanding of 'consumer welfare' in terms of short term price effects is not sufficient to capture and regulate the layers of market power in the modern economy. Specifically, this understanding fails to appreciate the risk of predatory pricing along with the integration of business entities across markets. This applies starkly in the context of platform economies as (1) The economics of platform markets encourages a company to pursue growth over profits, which has been rewarded by investors. (2) Often online platforms, like Amazon serve as critical intermediaries which allow them to integrate across business lines to restrict access to basic infrastructure that their rival depend on.

Indian competition law eschews the structural approach. Both Sections 3 and 4 of the Competition Act require the presence of an anti-competitive agreement or an abuse of a dominant position for a company to be held liable. Merely having a dominant position is not sufficient enough to attract the ire of the CCI. The CCI has held that Flipkart and Amazon have not abused their dominant position. A rethinking of the competition law regime that regulates the distortions caused by Amazon's loss-making strategies and related distortions is needed.

D – Small Enterprises and Start-ups

4.14. Integration of small enterprises and MSMEs in the digital sphere is important. In order to ease the process, of onboarding, for MSMEs and to provide them best practices, platforms, where they already exist, (like e-lala, Tribes India) will be strengthened.

Comment: *The strengthening of platforms such as e-lala and Tribes India is a welcome measure in terms of opportunities to small enterprises.*

E – Taxation Issues

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

²² Donald F. Turner & Carl Kaysen, *Antitrust Policy: An Economic and Legal Analysis* (1959); Joe S. Bain, *Workable Competition in Oligopoly: Theoretical Considerations and Some Empirical Evidence*, 40 *Am. Econ. Rev.* 35, 36-38 (1950)

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.

Comment: *The policy supports the concept of "significant economic presence" as a means of ensuring that income and profits made from activities in India is taxed in a better manner. The issue of international taxation is too complicated and nuanced for it to be so summarily addressed in an E-commerce policy. Addressing a complicated issue in such a cursory manner leads to solutions which may not be able to appreciate all the complexities of the issue, for e.g. there does not seem to be any discussion on how to deal with investments through tax havens such as Mauritius with which India has Double Taxation Avoidance Treaties and which are used by companies to avoid paying the appropriate rates for corporate tax. Therefore issues such as international taxation have no place in a policy such as this. If it is felt that in the context of the e-commerce industry, where non-resident companies control most of the market, that international taxation is a relevant issue, then the policy should limit itself to defining the problems that arise with the present tax system vis-à-vis such international companies.*

F – Consumer Protection

4.15. The atypical nature of an e-commerce transaction necessitates a consumer protection framework specific to this sector.

Comment: *The recognition of consumer issues in the context of e-commerce is a welcome step in the policy since the unique problems associated with ecommerce require an overhaul of the consumer dispute redressal mechanism of India which is rife with delays and overburdened with a large pendency of cases.*

4.16. India will move towards a system for electronic redressal of grievances including making available compensation to the aggrieved consumer electronically. It is only rational that a transaction completed online should have an online system of grievances redressal which will, in turn, boost consumer confidence. In this regard, mechanisms will be developed to establish e-consumer courts as part of the mission mode e-government project in order to address grievances online.

Comment: *E-courts have been suggested as a way of dealing with consumer issues in an efficient manner however one must recognize the fact that such e-courts may not be able to deal with all the issues arising out of e-commerce transactions, for eg. if physical evidence has to be examined, or cross examination of a witness is to be conducted,*

such actions cannot take place through e-courts One very useful change in the current laws which would be extremely consumer friendly for the e-commerce industry would be to enact a statute similar to the Unfair Contract Terms Act, 1977 of England which severely restricts the rights of the parties to limit their liability through exemption or disclaimer clauses.

4.17. Unsolicited commercial messages (on various platforms including but not limited to SMSs, emails etc.) and calls will be regulated. A legal framework for this will be developed.

Comment: *The requirement of regulating unsolicited commercial messages which would include messages apart from calls and SMSes is also a great initiative. The policy therefore recognizes the limitations of the current framework of TRAI which only addresses unsolicited SMSes.*

4.21 (G) Payment Related

The policy notes that issues related to payment processes will be addressed to ensure security. The Reserve Bank of India is responsible for developing appropriate security guidelines for the finance sector. E-commerce services processing payments would have to comply with these standards. We would recommend that the DPIIT coordinate with the RBI to ensure that security challenges facing e-commerce services specifically are addressed, but that the DPIIT does not undertake and develop security standards for payments applicable only to e-commerce services.

4.21 (H) Tracking the digital economy

The policy emphasizes the importance of public sector data, supporting Digital India and finding ways to leverage artificial intelligence towards informing policy making. Though we welcome the recognition and agree with the importance of public sector data - before turning to artificial intelligence to inform policy making, we would encourage the government to focus on developing a comprehensive data protection legislation that extends to the private sector and public sector, standardized data collection and storage, and defined guidelines for public sector use of AI.

4.21 (I) Exemption from content liability

The policy places the responsibility of ensuring genuineness of information and content on online platforms and social media. This responsibility speaks to intermediary liability. As India has an existing framework for intermediary liability under section 79 of the IT Act and associated Rules- we would recommend that issues around intermediary liability are addressed fully in the provision and Rules to avoid conflicting or inconsistent

requirements. Currently there are draft amendments to these rules and CIS has [submitted comments](#) to the same.

4.21 (J) Environmentally Sustainable Growth

The policy notes that a suitable policy will be devised to further the Swachh Bharat Abhiyan “reduce, reuse, and recycle”. It is a welcome step that the DPIIT will be requiring companies to find sustainable and environmentally friendly practices. Concerns around the impact of data centres and digital infrastructure on the environment and global warming are growing.²³

²³ Burrington I (2015), “The environmental toll of a Netflix binge”
,<<https://www.theatlantic.com/technology/archive/2015/12/there-are-no-clean-clouds/420744/>>