



Submission of Comments on DIPP's Draft E-Commerce Policy

Digital Empowerment Foundation



This work is licensed under a Creative Commons
Attribution-NonCommercial-ShareAlike 4.0
International License

To:
Department for the Promotion of Industry and Internal Trade
Government of India
Udyog Bhavan
New Delhi – 110011
Date: 29 March 2019

Subject: Submission of comments/ suggestions on the draft National E-Commerce Policy 2019

Dear Madam/ Sir,

The Digital Empowerment Foundation (DEF) wishes to thank the Department for the Promotion of Industry and Internal Trade of the Hon'ble Ministry of Commerce and Industry for the opportunity to submit our comments on the draft National E-Commerce Policy, 2019.

Digital Empowerment Foundation is a New Delhi-based not-for-profit organisation. It was born out of the deep understanding that marginalised communities living in socio-economic marginalisation and information poverty can be empowered to improve their lives by providing them with access to information and knowledge using digital tools.

We recognise unhindered and universal access to the internet as a key driver of development and empowerment amongst the digital excluded masses in India. We are grateful that the DIPP has sought greater clarity on the draft e-commerce policy.

My colleague, Ms. Anulekha Nandi, who has drafted our response, and DEF would be happy to provide any further support to DIPP on this issue.

Yours sincerely,



Osama Manzar
Founder and Director
Digital Empowerment Foundation
House 44, 3rd Floor, Kalu Sarai, New Delhi - 110017
Website: www.defindia.org
Phone no.: +91-11-26532787

General Comments:

The aim of the draft E-Commerce policy is an expansive one of economic transformation propelled by the expansion of the digital economy fuelled by data. It envisions an overhaul of the entire digital economic ecosystem to develop a regulatory regime that can drive economic growth by preventing market failures and distortions and promoting entrepreneurship and innovation. It attempts to do this by addressing six broad issues, that it deems, is characteristic of the ecosystem: (1) Data; (2) Infrastructure Development; (3) E-Commerce Marketplaces; (4) Regulatory Issues; (5) Stimulating Domestic Digital Economy; and (6) Export Promotion through E-Commerce. An Indian position on E-Commerce was also timely because of the WTO (World Trade Organisation) negotiations which aim to create binding obligations on member countries relating to e-commerce. **As a result of the multiplicity of inputs driving the policy formulation, the aims and objectives of the said policy are wide and over-reaching in scope.** As a result of this, it lacks the coherence required for a seamless implementation to meet the considerable challenges and create positive impact across its issue areas. This would have **serious implications for social and economic justice given that some of its prescriptions related to the handling, management, and use of data encroaches upon data protection mandates.** While it has been [argued](#) that an area can be regulated from different perspectives by different regulators and different agencies on the condition that they are mutually compatible it becomes important to reinforce that the requirement for harmonisation when the regulatory object, data in this case, is similar across different areas.

Out of the six issues that it identifies, it privileges data to be the most important driving factor that underpins all economic and commercial activities within the digital ecosystem. It sees access to data as the sole driver of entrepreneurship and innovations at the detriment of not giving adequate policy space to other facilitative factors that can stimulate entrepreneurship like access to funds, mentorship, access to infrastructures for innovation and experimentation etc. Proceeding from the understanding of data being the primary driver of economic growth within the digital economic transformations, the policy mandates restrictions on cross-border data flow and access to localised data to domestic firms. This, according to the policy, would counter the network effects enjoyed by big technology companies, which would also be contained via the data sharing by major technology companies. However, it is not clear whether what the modalities of such data sharing would be. Neither a company nor the Indian government own the data that would enable them to grant access rights to third parties, Indian or otherwise. It is also not clear what would be the ownership, control, and management of infrastructures to store localised data. Further, it is confounding to understand how the diverse data demands of diverse entities operating in diverse domains would be met. Who would take the decisions on the combination and aggregation of datasets to be shared with requesting entities? Moreover, what would be the modalities of the access granted to entities to the vast trove of data is to be localised and made available for domestic economic upliftment?

Any policy adopted towards economic growth driven by digital transformation should be cognisant of attendant issues and challenges that potentially impact on the distributive justice and social, economic, political and fundamental rights relating to the distribution of gains and dividends reaped from such transformations. Keeping this perspective in mind, this response aims to provide in-depth analysis and recommendations towards specific points of contention within this policy that would merit a closer look, debate, and deliberation.

Specific Comments:

- **The policy muddles the understanding of data ownership**

Context: The policy highlights the importance of data for emerging and evolving business models while mentioning the importance of data ownership and the need for the consumer/user to retain ownership rights over their data. One of its stated aims is to ‘streamline the protection of personal data and empower users/ consumers to have control over the data that they generate and own’ (p. 6). The policy understands data as a capital asset or intellectual property¹ and argues for the access by Indian MSMEs (Micro, Small, and Medium Enterprises) and start-ups to put them at par with major international technology companies which benefit from the volume of the data processed by them. ‘In the light of the increasing importance of data protection and privacy’ (p. 6) the policy aims to regulate cross-border data flow while enabling access to the anonymised ‘community data’ collected by IoT (Internet of Things) devices in public places. It reiterates that individuals own the rights to their data and use of such data requires their express consent going further to state that ‘(E)ven after data is anonymised, the interests of the individual cannot be separated from it. Data about a particular group will always have something of value for them’ (p. 14)’.

It then goes on to say that the data of a country is best thought of as a collective resource or a national asset that the government holds in trust but ‘rights to which can be permitted’ using the analogy of a natural resource mine or spectrum. Taking this understanding further, it goes on to state that India and its citizens have a sovereign right to their data through the conceptions of a data commons. The policy states that the issues under consideration in this policy pertaining to data are of a much wider scope than privacy and that domestic companies need access to such data to compete effectively within the digital economy to counter the network effects that major technology companies enjoy in relation to their first-mover advantage. This leads to policy prescription to regulate cross-border data flow and mandate data localisation. The latter through the location of computer facilities like data centres and server farms are hoped to give a fillip not only to computing in India but also local job creation.

The strategies to be adopted for taking advantage of digital gains include developing a legal and technological framework to regulate cross border data flow of community data and data generated by Indians via various sources. It further specifies conditions for a business entity collecting and processing data in India and storing it abroad in relation to making it available to other business entities and third parties even with customer consent. This includes further injunctions against sharing of the data with foreign governments, proving access to such data on requests made by Indian authorities, and stipulations for prescribed consequences (to be formulated by the Central Government) in case of non-compliance. The policy also lists exemptions for data localisation and formulation of a suitable framework for sharing of community data.

Analysis: The conceptualisations on data ownership and rights mobilised by the policy seems to work at cross-purposes with the principles of privacy and data protection.

¹ Cognisant of the conceptual distinctions between capital asset and intellectual property, herein it is used as described in the Policy.

- Though the policy self-admittedly aims to answer to a scope wider than privacy concerns, right to privacy and data protection regulations exist to contend with State over-reach and unfettered business exploitation. It would entail a state policy transgressing a proposed primary legislation.
- Though the policy states that interests of the '*individual*' cannot be divorced even from anonymised data it aims to develop a framework for the sharing of anonymised '*community data*'. This muddles the concept of who is the actual rights-holder, a community or an individual. Privacy and data protection principles identifies the individuals as the primary rights-holder. The e-commerce policy contributes to operational obfuscation of data protection regulations and principles. Community data is still a sum of part of data generated by individuals.
- It then goes on to identify data as a national resource that the government holds in trust by using the analogies of a natural resource mine and spectrum. This is problematic because data is dynamic and corresponds to individual rights that can be likened, conceptually, to property rights. If data is a national resource, does an individual citizen have an equal and inalienable right to data generated by their fellow citizen? If so, on what grounds. Moreover, the analogies themselves are problematic. A natural resource mine or spectrum is leased by the government to public or private entities for extraction or use which is then translated into a consumable resource through the process of production or service delivery. The final product whether it be in the form of energy or telecommunication services has to be purchased by the final user/ citizen from the entities producing or delivering these services. This would entail a double exaction from users. First, in the form of their data for the services provided by technology companies and further for the services rendered by other companies on the back of the data generated by users in the first place.
- The policy over-rides individual capacity to give consent in two instances: First, when it says that the Government holds the data of the citizen in trust it takes over an individual's capacity to give informed consent to the uses to which their data might be put. Second, with 1.2 (a) and (b) it states that sensitive data² collected and processed in India and stored abroad shall not be made available to third parties and other business entities outside India even with customer consent. This adopts a paternalistic approach and negates the cornerstone of data protection regulations that respects the autonomy and the capacity of the individual to give informed consent to the uses to which their data might be put. The autonomy to give informed consent is a foundational signifier of ownership rights that an individual has over their data.
- The policy says that data of a particular group will always have something of value for them. Groups can constitute of women, men, marginalised communities and identities etc. It is not clear whether the policy intends to homogenise groups with monolithic group identities and ignore the plurality and complexity that makes up an individual identity as a sum of parts making up social life.
- Treating the data of Indian citizens as a form of commons also suffers from concomitant problematic of the tragedy of the commons in which individual actors

² It does define or specify the categories of sensitive data. Given, that it diverges significantly from the proposed data protection framework, such definition and identification of categories become important.

acting in their own self-interest act against the collective good flowing from the common resource, thereby collectively negating the value of the commons.

- The concept of sovereign right over the data generated fails to qualify whether it corresponds to the sovereign right of the individual over the data generated by them or the sovereignty of the Union of India over the data of the citizens that it claims the country holds in trust.

In sum, the policy prescriptions work at cross-purposes with the objectives as well with complementary developments in the area of right to privacy and data protection framework. These frameworks are contingent on clear and unclarified ownership rights of an individual over the data generated by them. Obfuscating the operation of such rights in practice as some of the provisions in this policy translate into doing, has serious implications on the exercise of such rights by individuals.

Recommendations: In order for the e-commerce policy to take a balanced approach it is important that it is harmonised with highest standards of rights-protective data protection principles and frameworks available. This will ensure that the pathway to economic growth and civil liberties are complementary and not mutually exclusive or oppositional. This will aim to ensure not just economic growth and development but economic and social justice to individual citizens.

- **Ambiguous definitions, objectives, standards and categorisations**

Context: The policy aims to cater to domestic entrepreneurs and leveraging access of MSMEs, vendors, and traders to the digital ecosystem and data. It cites instances of the Aadhaar biometric system, the Bharat Interface for Money (BHIM), e-Know Your Customer (e-KYC), and Goods and Services Tax (GST) Tax network as well as the Right to Information (RTI) Act as a pathway to citizen empowerment, the next step in which is to give citizens control over their own data. It further identifies different categories of data such as individual or community data. It holds that India's data should be used for the country's development and that Indian citizens and companies should derive the economic benefit arising from monetisation of data. In order to deliver on this, it suggests that a suitable framework is to be developed for sharing community data that serves 'larger public interest' with start-ups and firms. Curiously, it then goes on to say that 'public interest' and 'public good' are evolving concepts. Further, that the implementation of this policy prescription is to be undertaken by a 'data authority' to be established for this purpose. In order to achieve its objectives within the existing ecosystem, it outlines the need to take steps to develop capacity for data storage in India. This will go in tandem with developing domestic alternatives to foreign-based cloud and email facilities and providing budgetary support for the same. It also highlights the benefits that have accrued to consumers through 'access to greater variety of products at competitive prices' and how it has led to the expansion of employment opportunities. However, it then goes on to say that network effects have led to market consolidation leading to monopoly prices and raising barriers of entry for new entrants. Moreover, it tasks the Department of Post to conduct due diligence on the misuse of the gifting route and misuse of the Foreign Trade (Development and Regulation) Act, 1992 as well as the services that it can potentially provide to the logistics sector which is an indispensable component for the growth of the e-commerce sector.

Analysis: The lack of clarity on policy prescriptions leads to a flawed operationalisation and implementation of principles, thereby disadvantaging the intended constituents of the policy.

- It is a curious position to club the Aadhaar biometric system, the BHIM UPI, e-KYC, GST network, and the RTI Act together as India having its own sources of data. With the exception of the RTI Act, a public accountability tool, it is not sure whether the rest is a stand-in for reviving the use of the JAM trinity, or some similar formulation thereof, to aggregate sensitive personal data from across various government sources in order to make it monetisation ready, as was proposed in the previous iteration of the draft e-commerce policy.
- It identifies different categories of data such as individual and community data without adopting the categorisations put forward by the data protection bill. As a result of this it fails to prescribe different handling requirements for different data categories and serves to work at cross-purposes with the provisions and principles of the data protection bill.
- It mentions that Indian citizens and Indian companies should derive the benefits from the monetisation of the data generated in India. However, the policy uses domestic companies, MSMEs, vendors, traders, and start-ups almost inter-changeably without clarifying what would be benchmark for companies to qualify for access to data. The previous policy had mentioned that start-ups that meet a specific idea i.e. turnover of over Rs. 50 crore would qualify for data access. This is counter-intuitive since the stated aim of the policy is to support those entities who would not be able to take advantage of the network effects that big companies enjoy. Arguably companies with over Rs. 50 crore in turnover have achieved sufficient scale to leverage the network effects that they have monetised into such revenue. Moreover, it does not mention whether the companies would lose access to government incentives in terms of access to such data once they have achieved a certain scale. This is an important point to meet the stated objective of levelling the playing field and avoiding the replication of industry consolidation in India that has happened internationally.
- It mentions ‘public interest’ and ‘larger public good’ without prescribing suitable tests and due process to determine such. Moreover, mentioning that these are evolving concepts is overreaching and provides sufficient latitude for abuse of power and arbitrary policy, rules, and regulation without the concomitant need to have a substantial evidence base to validate such agenda-setting and prescriptions. Moreover, to keep in line with the mandate of the Department and the e-commerce priorities it is important to define what public interest and public good mean in relation to the digital economy so that neither the Department nor the policy goes beyond the ambit of what it is mandated to regulate.
- The policy outlines that a ‘data authority’ would be established for the purpose of ensuring adherence to ‘public interest’ and ‘public authority’ and providing access to data for ‘start-ups and firms’. It is unclear about the extent to which the remit of this ‘data authority’ would be distinct from the Data Protection Authority prescribed under the Data Protection Bill or whether or not they would be one and the same individual/entity.

- Admitting the positive impacts that e-commerce investments have had on the Indian economy and then trying to increase the cost of operations for those very same entities through regulations on cross-border data flow, data localisation, and mandatory disclosure of source code does not take into account how the resulting impact on consumer welfare (through a rise in prices) would be accommodated. A policy grappling with competition issues would have to provide steps to be taken to balance the knock-on impact of policies to control the impact of deep discounting and predatory pricing.
- The policy outlines the Department of Post as an important stakeholder in the ecosystem. In what looks like an inspiration from how the US Postal Service was resuscitated through partnership with Amazon, adding critical due diligence functions and infrastructural responsibilities without proper assessment as to whether it has the capacity to undertake and deliver upon such expectations, without institutional capacity-building would be detrimental to the ecosystem.
- The policy also mandates the provision of access to data stored abroad to Indian authorities upon request. However, there is a lack of a due process and judicial oversight for such processes that will also need to answer to the compliance requirement of the countries in which the data is stored.

Recommendations: The lack of clarity in definitions and categorisations obfuscates transparency and public accountability on practices that can have a serious impact on individuals' social and economic rights.

- Delineate evidence-based rationale that prevents an Indian start-up to get market access given the success of India brands like ShareChat, Swiggy, Ola etc. without mandating privacy encroaching access to data.
 - Establish transparent and accountable due process for the use of individual data stored in government databases. This includes any decision regarding combination of databases to derive derivative databases or insights.
 - Clarify objectives and streamline prescriptions with relation to market consolidation and give equal weightage to market consolidation by domestic firms as by international firms.
 - Develop an evidence-based analysis on market consolidation and targeted policy interventions so as not to cast a wide net with a trawling effect on other market dynamics and individual rights.
 - Undertake research and analysis of the digital ecosystem to identify areas of growth which would benefit from targeted policy intervention.
- **The policy does not highlight a concomitant business responsibility towards data rights**

Context: The primary driving force behind the policy is to make data generated in India available to the Indian companies and firms in order to enable them to partake in the digital dividends that big data offers within the digital economy. According to the policy, India is a

treasure trove of large amount of commercially available data. However, the economic benefits accruing from this data seems to disproportionately benefit international technology firms which forecloses the ability of Indian firms to create high value digital products without access to such data. It identifies monetisation of data through regulation of cross-border data flows and data localisation as the enabler that can bring about internal economic equitability within the country. The policy makes a case for privileging the access to consumer data for domestic firms vis-à-vis foreign firms.

Analysis: The policy frames the access to data for companies in terms of levelling the playing field on account of network effects that cause major technology companies to amass huge amounts of data that help them to consolidate their position across national and international markets. Given the significant flow of benefits to domestic corporate entities envisioned in the policy, the policy does not create obligations on business to develop security protocols for accessing the data that will translate into economic dividends from them. Given that the policy understands data as a capital asset, individuals are both the owners of capital invested in domestic economic activity as well as consumers of the products and services produced through the use of data by domestic technology companies. However, there is no positive consideration flowing to individual data owners under this conception which results in double exaction of both the capital resource from the owner as well the payment towards the services they would avail from entities which translate such capital into products and services.

Though the policy identifies both Indian citizens as well as businesses as direct beneficiaries of the monetisation of localised data, it does not extend the corresponding dividends arising out of such activity on to the individual citizen in the same way it privileges business entities. When businesses profit from ‘capital’ resources provided by individuals, it becomes imperative upon them to adopt ethical rights-protective practices so that they do not function to the detriment of users, at the very least. The policy identifies the increased mainstreaming of artificial intelligence and how localised access to data will emerge as a main determinant of success of an enterprise in the digital economy. Given the potential for data discrimination within data driven models, the policy does not contain provisions that enable individual users to seek remedy, accountability, and transparency through competent channels and with competent authorities in case of adverse business activities that individuals might be a victim of. The policy does not empower users through grievance redressal mechanisms nor delineate obligations on businesses to due diligence within their artificial intelligence and machine learning processes.

Recommendations: Given the potential for pervasive discrimination within data driven systems perpetuating inherent biases it is important for businesses to have dynamic human rights policies that is reflective of the interaction between technology and human rights.

- Make it incumbent upon e-commerce companies to have a human rights policy along with grievance redressal mechanism in line with international standards the United Nations Guiding Principles for Business and Human Rights.
- Data transaction within the current digital ecosystem takes place as an exchange of services in return for individual data. Under the present system, there is no system of exchange but unilateral provision of data to business entities without a direct corresponding return in services. This disprivileges an individual to take an informed decision about whether to provide their data for a particular service. Therefore, it is advised that the current proposition of providing domestic business entities with

access to aggregated and combined databases should be dropped in favour of creating a facilitative environment for nascent domestic industries through other policy measures like providing access to funds, infrastructure, and equipment for experimentation and innovation. This would allow domestic industry to be a competitive force and avoid excessive state dependency, thereby instituting and injecting economic sustainability for the long run.