Critical Areas of Response to the Draft E-Commerce Policy

Submission by The Dialogue

Introduction

The Dialogue would like to take this opportunity to thank the Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce, Government of India, for carrying out the Consultation Process on the Draft E-Commerce Policy. We welcome the intent of the Government to support and enhance the e-commerce sector in India and hope that our submissions help the Government towards making an informed policy decision.

India is the world's fastest growing e-commerce market. India's e-commerce sector has experienced exponential growth in the last decade, up from USD 3.8 billion in 2009 to USD 38 billion in 2017. The growth is expected to continue in the near and long term. The e-commerce market is expected to reach USD 64 billion by 2020 and USD 200 billion by 2026 from its current size of USD 38 billion.

Driven by a young demographic profile, mobile revolution, growing internet penetration in tier-II and tier-III towns and a multitude of other factors, the country's e-commerce market has attracted large investments, resulting in an exponential growth of the sector. As the sector grows, it is important to create a supporting

policy regime and provide a fair regulatory environment for different players in the sector.

The vision for this policy states that it has been drafted to create a level playing field for all stakeholders including individual consumers, MSMEs, and startups. However, the government has the responsibility to pursue a development agenda while preventing market failures and distortions.

Creating a conducive policy environment is key to maintaining a sustainable growth of this sector. The policymakers should strive to balance the interest of the consumers, suppliers, online vendors, e-commerce companies and other players in the value chain, while ensuring that the policies serve the economic interest of the country.

As part of the consultation, The Dialogue conducted a Stakeholder Roundtable in the first week of March on the draft policy and we have included the inputs collected from the meeting. In our submission we have looked at various themes that are covered in the Draft Policy and address all such areas with our inputs and suggestions.

1. What should be the definition of E-Commerce?

The Draft Policy defines *'E-Commerce' as including buying, selling, marketing or distribution of…. digital products and services through electronic network.'* This particular definition encompasses any type of online transaction, which is beyond the scope of e-commerce transaction. Transactions pertaining to booking of ticket, cab, etc. would also constitute as e-commerce. Any electronic transaction cannot be constituted as e-commerce. Therefore, we recommend the concerned department to narrow the definition of e-commerce to only those online transactions that are in line with agreed principles of electronic commercial transaction.

2. Are the issues of data ownership beyond the scope of the Draft E-Commerce Policy?

The Draft Policy on e-commerce discusses issues ranging from cloud computing to search engines, emails, Internet of Things, localisation etc. Quite a significant portion of the Draft E-Commerce Policy focuses on areas that have been addressed, or are a matter of conversation of the Data Protection Bill, 2018 and other laws and policies. The Bill is a result of a long consultative process on areas concerning privacy, cross-border data flows, data ownership and access. To introduce a separate policy document on similar lines meant for a different purpose seems disjointed and conflicting in nature with the original purpose of the Data Protection Bill. We therefore recommend the Government to narrow the focus of this policy to issues related only to e-commerce.

3. Is data a natural resource?

Unlike oil, data is not naturally occurring and therefore cannot be classified as a 'natural resource'. It is the result of technological investment based on the relationship between consumers and fiduciaries. Unlike oil, it is infinite, and the global volume of data generated continues to grow, while at the same time, it can be duplicated by multiple organisations, as the same data set, through different technologies, can be processed differently to generate parallel insights.

4. Who owns the data?

It must be made clear that the citizen, the people, own their individual data. The Draft Policy does talk about this at the beginning of Page 14 of the document. Since data is owned only by the customer, then it must be his/her prerogative to use the data in ways he/she deems fit. Therefore, data should only be processed with the explicit consent of the user, which is also mentioned in the Data Protection Bill, 2018. Any fiduciary, be it the government or

corporation is a mere custodian of such data. While the individual owns her data, the corporations process it using technology and in return provide digital services and products. There exist no other concepts around ownership and custodianship in this respect. Indian data, generated from the people of India, belong to individual Indians who have the power to control the flow of their data.

5. Should data be held as a 'collective resource'?

The Draft E-Commerce Policy talks about "*data of a country, therefore, is best thought of a collective resource, a national asset, that the government holds in trust, but rights to which can be permitted* "and compares it to a 'societal commons. We welcome the intent of the government to identify solutions to our socio-economic challenges with the power of data. The method in question however is an incorrect assumption. This directly contradicts both the views of the Hon'ble Supreme Court, as well as the views of the Committee of Experts on Privacy. The role of the government should be limited to protecting rights of citizens, and not placing any further restrictions on such rights.

Let us address how data ecosystem works. Since the rise in digital services and the telecom boom that provided internet access to people of India, online services, products and apps have transformed the way we go about our life. Be it transport, healthcare, education, finance, payments or banking, the power of digital services and data has brought a new dimension which nobody could have predicted just a couple of decades ago. The surge in digital products was propelled with cutting edge processing technologies that was deployed in many instances by the private sector. Such technologies, with personal data as an ingredient, developed high-level insights, that were subsequently analysed to provide consumers with even better services. For example, cab aggregator services have played a tremendous role to solve key transportation challenges in India. Millions throughout the world are benefitting from the business models of cab aggregators that enabled affordable and convenient modes of transport. As they spread their services across multiple communities, cities and jurisdictions, they subsequently developed high-level insights about the travel patterns of commuters, busiest hours on the roads, the fastest and slowest routes etc. Such insights are a key to understanding the ecosystem that help them improve their services. Moreover, these insights, or wisdom about a community's behavioral patterns did not come about only through collection of personal data. It was developed using technology that required investment and infrastructural and logistical costs borne by the private players, along with a service they provided to the consumers. In many ways, these insights may be classified as an

intellectual property, or wisdom, of the organisation. Additionally, insights would not be useful if a service is not provided against it, as the purpose of developing this knowledge is to enhance the end user experience.

The concept of Community Data is contrary to the way the present ecosystem works, where societal benefits merge with commercial business models based on the power of data. To ask for insights would be counter-productive for India. For the government, or any other private or public entity, to ask for insights from an organisation, without having made the investments into the technology, and without providing the services, would set a dangerous precedent for India in the future. If an organisation believes that other entities may have access to their data sets and insights developed over years of technological investment, it would send a discouraging and demotivating message that may hamper the spirit of innovation and competitiveness in the Indian market. The return on investment would fall.

What India should be doing instead, is to incentivize startups, new tech, to develop technologies that can process our citizen's data by providing them with cutting edge, valuable services. Through this approach, Indian companies will develop smart insights that could help them enhance decision making. Once the ecosystem of home-grown internet services develops and matures, it could create a thriving data economy in India. For India to take the leap towards becoming a major data superpower, innovation into high-end products and services that meets our societal challenges is the way to go about it.

6. Restricting cross-border flow of data generated by Internet of Things (IoT) devices and of data generated in India

The Draft E-Commerce Policy states that it seeks to create a legal and technological framework to restrict cross border flow of data generated by Indian users and data collected by IoT devices.

It is well understood and appreciated that government access to data for law enforcement is paramount for national security. However, to assume that access of data depends on the location of data, is an incorrect assumption. On the contrary, placing restricting on the flow of data across borders can place unnecessary costs on business. The Dialogue did a comprehensive study on data localisation[1] and cross border data flows, in November 2018, and the research

[1] Data Localisation in a Globalised World: An Indian Perspective, The Dialogue http://thedialogue.co/dialogue/wp-content/uploads/2018/12/Data-Localisation-in-a-Globalised-World.pdf

revealed that localising data generated in India will increase the costs burden on businesses and customers in India, will not fulfill India's quest for lawful access to data and will isolate India from global technological progress. This could reduce foreign investments and thereby place hurdle on India's efforts to emerge as the leading economic success story. It will isolate India's economic activity with the rest of the world and could also remove Indian data from global data sets, which could potentially harm India's AI progress. IoT and interconnectivity is essential to realize the potential of fourth industrial revolution and the transformation it will bring to public services, such as transportation, healthcare, education, financial services etc. The Prime Minister's dream of creating smart cities will be based on the power of interconnected services. However, limiting cross-border data flows might remove global investments and the value global data sets could bring.

Localising of data in India will also limit the potential for India to compete in the global markets. Free flow of data across borders is paramount to enable digital services. It will cut-off India from fraud detection, patterns of fraudulent activity that are collected from across the world and analysed in a centralized location help improve fraud prevention tech. Government should instead focus on ensuring robust practices to protect data and place enough checks and balances as well as safeguards for ethical use of data. Internet should not be fragmented and split into boundaries and we should follow high standards of security. Restriction of data will reduce innovation, sub-optimal standard of service, increase cost, reduced competitiveness of Indian firms globally.

Studies have also revealed if India were to introduce an economy-wide data localization measure, the impact would increase to -0.8%. Besides, it would also hit India's projected growth by approximately 20%. Regarding investments, exports, and long-term growth, a blanket data localization measure would result in a 1.9% drop. Losses in welfare alone could reach as high as $3.1–14.5 billion. To give perspective on what it might affect the average Indian, the adverse welfare effect would cost an Indian worker almost 11% of their average monthly salary[2].

Another likely bi-product of the increased costs and lowered efficiency is the reduction of the global reach of organizations. Data location laws can not only deter but can also act as causes for organizational exit from countries. Should a private entity no longer consider costs to be worth the benefits it gets in return, operations in that country can cease to exist. The direct impact on the firm is the reduction of scope, leading to

[2] "THE COSTS OF DATA LOCALISATION: FRIENDLY FIRE ON ... - ECIPE." http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

reinvesting the capital invested initially. However, the brunt of the exit might be felt on the host country, and more specifically, their citizens. Companies ceasing operations on regions can mean jobs lost for hundreds of workers. On the consumer side, it might mean the lack of options. For the industry, it might mean the exit for a competitor, for better or worse.

In many cases, it is not possible to process all data locally and maintain the same quality of service as could otherwise be achieved (for example, round-the-clock, follow-the-sun customer service). This is essential for companies that operate globally and follow different markets/

The trend towards micro-services in service architecture and increasing distribution of data processing means that data localization restrictions are likely to result in companies choosing not to serve the Indian market or significantly reducing the functionality of their services.

Additionally, India has gradually moved towards making digital and cashless payments a mainstream reality for its population. For a country that wants to move on from cashless payments, better financial services are a necessity. There is a tremendous scope for digitization within India's center as well as the periphery. There is a demand for more straightforward methods of payment. The success of alternatives to traditional banks proved the same.

Data localisation will be a step backward for the digital payments industry. Not only would it make it costlier for international banks to operate, but it would also reduce the incentive for them to innovate and try out new forms of payment on the front and back end. 'Black money' has been a critical issue for India[3], and a push for digital and cashless transactions is a tested, long-term alternative to the same. So, in a time where better financial services can be support development, slowing down their expansion through data localization will deter the cause that the government has been championing.

Localisation will also make Indian data vulnerable to global cyberspace attacks. Security is not enhanced just because data resides within a particular jurisdiction. Security is a function of the technical, organizational, and financial capacity of an entity to protect the data and provide physical protection for a data center[4]. So

[3] "Black Money and Politics in India | Economic and Political Weekly - Epw." https://www.epw.in/journal/2017/7/special-articles/black-money-and-politics-india.html.

[4] "Data Processing and Security Terms | Google Cloud Platform Terms ...." 7 Feb. 2017, https://cloud.google.com/terms/data-processing-terms-20170207.

instead of storing data in centers around India, security would be better facilitated with the creation and use of de-centralized and end-to-end encrypted services that do not store all consumer data in one place.

While at the same time, we understand that the Government would want a robust data center industry in the country. To achieve this, Government should incentivize and encourage companies to store and process India, rather than forcing them to do so. By placing due process of law, adhering to high levels of privacy and complying with international standards of security, Government should seek to create India the most rewarding destination for data processing.

Moreover, our research suggests the following procedures must be adhered to if data is stored in India, along with a due process of law in place.

(i) Technical Measures – prescribing the standards and specifications that need to be complied by the data processors and data fiduciaries. There must be enabling provisions to prescribe the standards and specifications as they evolve[5].

(ii) Physical Measures – prescribing the physical conditions viz., location, situation, construction, layout, etc., of the centers where the data is to be processed.

(iii) Access Control – regulating the process and authority for access to and handling of the data being processed.

(iv) Disaster Management & Recovery – prescribing the specifications for recovering and damage control in the event of a breach or disaster situation.

7. Should data flow be restricted even if consumer consent is given?

The Draft E-Commerce Policy proposes to *"prohibit the transfer of data stored overseas from one business entity to another, even with the consent of the customer"*.

Consent is key for data to be shared. This goes against the principle of the Supreme Court judgement as well as the Data Protection Bill, 2018. Removal of consent takes away a critical part of the privacy process that threatens misuse and abuse of data, which also goes against the *Puttuswamy* judgment guaranteeing the right to privacy. It also limits the control an individual would have over his/her data that could also harm the security of such data. It would also limit

[5] "Articles & Publications AUGUST 2018 - Induslaw." 3 Aug. 2018, https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf.

the advantage Indians could seek from such third-party transfers, especially in critical services such as healthcare, where data processed from different countries can provide better and affordable digital solutions to people.

8. The 'Network Effect'

The Draft E-Commerce Policy raises concerns about the 'network effect' that in the present era of data collection and processing, the larger the firm, the greater the access to potential sources of data and greater the likelihood of its success. Such conclusions are drawn without evidential support and states that 'selling at a loss' amounts to 'capital dumping', which is 'anti-competitive' in nature. The present business models in the internet and data era focus heavily on capturing market share and provide customers with the most affordable services. Such practices are not anti-competitive in nature but they help firms to provide better services with the latest technologies. The power of insights helps firms leverage their position in the market and such insights are a result of years of analysis, investment and innovation. Not only the consumes benefit with respect to availing cutting edge services, it also provides incentives for companies to innovate.

9. Should investments in Inventory model be limited?

The Government has limited foreign investment in the 'Inventory' model following on from the December 2018 notification. This would limit the choice to consumers and may also lead to higher prices. Moreover, the Government has exempted Indian companies from this prohibition, and has therefore allowed domestic companies to function in the 'Inventory' model. The difference in approach may have its implications with respect to foreign governments placing similar restrictions on India, sending a message of explicit protectionism, potentially discouraging future investments as well as potentially discriminating for MSMEs, startups and small vendors.

10. Privacy Vs. Economic Perspective

The Draft E-Commerce states that *"this is not just an issue of privacy. A comprehensive framework for protecting privacy of Indian citizens is under way with the draft Data Protection Bill. However, the issues under consideration in this Policy are of far wider reach."*

The Supreme Court through its judgment in 2017 granted the 'right to privacy' to all citizens of the country. The human rights debate flows from this judgment where privacy is now a fundamental right, therefore, this issue sits at the core of why digital rights perspective is crucial to the larger data debate. While spectrum

has been created by man and oil is a natural resource, the same cannot be stated about data.

Therefore, policies around e-commerce and data protection cannot be bifurcated and consultations need to happen side by side. Community data at the end of the day can be 2 things:

1) Intelligence

2) Anonymised Data

Questions around anonymized data are there with respect to that is there any privacy by design framework which is established or not. The personal and commercial interest have to be balanced with each other, which is an important aspect that should be addressed when such policies and laws are drafted. The most seminal document on data governance is the *Puttaswamy* judgment. According to the court ruling, the individual owns the data and how should it be used. It also talks on the centrality of the consent. The separation between privacy and economics is not possible. The Srikrishna Committee Report casts an obligation upon data fiduciaries as to how can they collect and process the data and that needs to be respected.

11. Should anonymized data be regulated?

Seeking to regulate anonymized data goes against best practices across data protection laws in various jurisdictions and is also inconsistent with India's Personal Data Protection Bill, 2018. Today, India's entrepreneurs need to test various AI and analytics models using anonymized data. These tools may not be available in India. Anonymization is a tool being used the world over to ensure privacy while at the same time extract valuable insights from the data. We recommend that in the interest of developing the digital ecosystem in India, including AI, the Draft Policy should not seek to impose any regulations in respect of such data.

12. On 'Sunset Clause'

The major market that the various e-commerce websites have captured is through offering high discounts. Under the Draft E-Commerce policy, the government has now decided that it would curtail this trend.

A sunset clause is one which defines the maximum duration of differential pricing strategies (such as deep discounts) that are implemented by e-commerce platforms to attract consumers. Once the sunset clause has been placed, it would be quite difficult for the online platforms to attract new customers as there is no denying that it is the huge discounts offered that keep the business of the e-biz going.

These changes come two months after the government modified the regulations governing Foreign Direct Investments in the country. As the overhauling process as proposed in this draft is set to cost a fortune to the e-commerce

companies in restructuring their Indian operations, this is set to cause major disruptions, which may lead to limited choices and costlier products to the consumers.

13. Should Source Code of Data be disclosed?

The Draft E-Commerce Policy seeks "*disclosure of source code for facilitating transfer of technology and development of applications for local needs as well as for security."* We believe that this requirement could have significant business ramifications for India. Source code is an intellectual property of IT companies that use it to develop applications, services and products, and which is a unique ingredient that is proprietary in nature. Seeking disclosure would undermine innovation, discourage businesses and may isolate India from the rest of the world in terms of application development, as businesses would feel threatened to give up proprietary information for market access. India may be left out from taking advantage of latest technological development as companies may opt out, keeping in mind that their most fundamental information on which they build technology could be disclosed in return of selling products and services in India. A

Such policies could be counter-productive with respect to India's economic interests.

14. Is the Draft E-Commerce Policy giving preferential treatment to domestic entities?

The Draft E-Commerce Policy throughout the paper seems to encourage preferential treatment of domestic entities. We at The Dialogue believe that Indian players and companies should compete with the best in the world and we support the growth of Indian companies to maximise the potential of the market. However, free market must be the basis of such competition. Indian companies must compete with foreign multinationals on equal terms and footing, and any preferential treatment may give them an advantage in the short term, but could be counter-productive in the medium to long term, especially when Indian companies invest abroad and seek access to international markets. Our domestic policies sheltering Indian institutions may undermine Indian companies' growth internationally, as other countries may impose similar market restrictions on Indian entities.

Such preferential treatment may also raise questions with respect to India's commitments under the GATT and the GATS.

With respect to payments, the policy mandates e-commerce entities to use RuPay on all e-commerce websites. The provision of the draft policy which mandates the online platforms to

compulsorily add RuPay as a payment method is arbitrary and infringes the sellers and retailers' right to carry out their business according to their wishes. It creates an unlevel playing field for other card operators and limits choice to consumers. The government should allow for competitive products in financial transactions. Such intentions seek to provide preferential market access to local players and may discourage foreign companies to operate in India, thereby undermining foreign investment and economic growth. Moreover, the National Payments Corporation of India (NPCI) has been acting as both regulator and market player in the payments sector, which is discouraging for the ecosystem and potentially gives NPCI a preferential advantage.

Similarly, mandating local presence for all companies operating in the Indian E-Commerce market may significantly increase costs and could impact their business.

Moreover, the policy states that *"domestic alternatives to foreign-based clouds and email facilities will be promoted."*, which is a clear sign of preferential treatment and may impact consumer choice and user experience, as well as affordable storage for startups.

Under the Hon'ble Prime Minister's Digital India initiative, the government seeks to make India a global success for technological progress. As the country looks outward to take India forward, preferential treatment may limit India's own objectives. Digital services and technologies are a matter of global competency, where one nation alone is not capable enough to keep track of latest innovation and development. Countries are interdependent on each other and require each other's expertise to provide better services to customers. Domestic preferential treatment will limit India's access to innovation and latest technology and may isolate India from participating at the highest levels. It may also limit choice to consumers.

15. Should Indian companies be allowed to access 'huge trove of data'?

The Draft E-Commerce Policy states that *"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."* It also states that *"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 policy risks walking a difficult path of breaking privacy and data protection for the sake of granting access to data and insights to Indian companies. First, we need a data protection law that provides the framework for privacy in India, and any transfer of data should flow from the

law and not the E-Commerce Policy. Second, such an intention would certainly discourage businesses to invest in India, undermine India's data protection initiatives and isolate the country from the rest of the world. Globally, countries are looking to safeguard data and develop due process of law for data access and sharing. With such policies, India seems to be moving on the opposite path of enabling 'unfettered access' for the sake of global economic competence and national security.

Any data that is collected, processed or shared in India should flow and be governed from the principles of consent, purpose, storage limitation and grounds for lawful processing. The Justice Shri Krishna Committee and the Data Protection Bill, 2018, have outlined this clearly. The E-Commerce policy seems to conflict such principles and we suggest that the purview of data protection and privacy be kept out of the ambit of the Draft E-Commerce Policy.

Additionally, in our research on data localisation, we stated that location of data has nothing to do with access. Merely hosting data in a particular jurisdiction does not increase the lawful access of such jurisdiction to such data, primarily due to conflict of laws from jurisdictions in which parent organization that may have custody, ownership, and control over such data are registered, the location of encryption keys, etc. Further, it is well documented that even currently, access to data for lawful/legitimate purposes is enabled and made possible without a requirement of the physical location of data. In the cloud era, countries that honor baseline principles of privacy, human rights, and due process should be able to efficiently access data (irrespective of where it is stored).

Since the data has been processed by a foreign company, which may be subject to the laws of the country where it is incorporated, there may be an inevitable conflict of laws situations. In order to minimise and avoid potential conflicts, while legislating in domestic laws, it needs to be kept in mind that domestic laws relating to privacy and data protection comply with established principles of international law. Therefore, rather than forcing foreign companies to share insights with their Indian counterparts, Indian government should encourage and positively incentivise Indian companies to develop products and services that can help them compete with international players that is in line with international economic and privacy principles and adheres to the philosophy of free-market dynamics. There is a need to develop capacity and capabilities of Indian companies and startups to access and process data in return of providing cutting edge services to Indian customers.

Conclusion

As India moves forward towards becoming a leading digital economy, it is imperative that our policies are designed in such a way that they provide equal footing and opportunities to all market players, the best and most affordable services to the consumers, creating enough jobs in the process and enabling India a hub for global technological progress. We believe that the vision of Digital India and making India a Five Trillion USD economy will require a consistent and sustained policy approach that incentivises local businesses to flourish while providing enough mechanisms to attract and protect foreign investments. It is fundamental to our progress towards becoming a developed nation that our policymakers strike this balance as one without the other may not help us achieve our long term goals.

About The Dialogue

The Dialogue is an emerging public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

Our aim is to enable a more coherent policy discourse in India backed by evidence and layered with the passion to transform India's growth, to help inform on public-policies, analyse the impact of governance and subsequently, develop robust solutions to tackle our challenges and capitalise on our opportunities. To achieve our objectives, we deploy a multi-stakeholder approach and work with Government, academia, civil-society, industry and other important stakeholders.

Contact Details:

Kazim Rizvi, Founding Director

Kazim.r@rthedialogue.co