ANNEXURE

AMCHAM SUBMISSION ON THE DRAFT NATIONAL E-COMMERCE POLICY

Definition of e-Commerce:

- In the modern era, most transactions are electronic, ranging from payment of school fees to paying for movie tickets. Having such a broad sweep definition is not in alignment with the commercial realities of electronic/digital transactions in modern times. Electronic/digital payment is only a means of payment. The broad definition will cover all cloud, telecom and Government services and make them e-commerce services.

  To avoid the legal anomalies that may be created by such a broad definition of e-commerce, it is recommended that the term should be narrowly defined to e-commerce as understood in the FDI policy using the twin parameters of e-marketplace and inventory model. Cloud services, citizen services by Government, intermediary services etc. should be kept out of its purview.

- The scope of this policy is all encompassing impacting a wide range of entities that include e-commerce platforms and sellers, Internet of Things, Search Engines, ISPs, Content ecosystem, as well as the larger Indian IT Industry who process data on behalf of clients. This policy therefore would be impacting the complete digital ecosystem in India, going much beyond its impact on online retail transactions to include for example a bank in India outsourcing its IT operations to a technology company, and complying with the RBI guidelines while doing so. Or A large corporate group procuring additional cloud services outside India

  As can be seen, these are all very different scenarios, catering to different end-users with different levels of sophistication, and a nuanced and calibrated approach is called for.

  The scope of this policy should not overlap with the other legislations such as Data Protection Bill, Consumer Protection Bill, RBI Guidelines, etc. which are already in advanced stages of finalization.

DATA related comments & suggestions:

- This policy focusses heavily on data. It is important to look at different types of data related issues and keep the appropriate types of data outside the purview of this policy, following the global standards.

  Classifying Data as a National Asset: Historically, the concept of National assets came about in order to conserve finite natural resources and prevent unscientific and unsustainable exploitation of the same. The intent behind the designation was to conserve such resources for a longer period to meet societal needs. Data, however, is an infinite resource. To give an analogy, while oil can be considered as a National asset, solar radiation and wind cannot be classified as a National asset (though both can be used to produce energy). The very concept of classifying data as a National asset is flawed, similar to the concept of "community data".

  State overriding individual rights (consent): The Draft Policy seeks to grant primacy to Government control over data – to the extent that it seeks to prohibit consent-based disclosure

of user data. This position of granting primacy to Government rights conflicts with the position of law in the Puttaswamy case, which grants primary rights to users to control dissemination of their data. Further, the Draft Policy considers it a "basic premise" that companies do not own rights over data that they process and monetize. This position should be reconsidered in light of realities of initiatives, innovation and modern business models.

Enterprise (business) and consumer data: Enterprise data should be clearly and completely kept out of the purview of this policy, where the focus should be on consumer data. Mixing them could have unintended consequences of destroying India's digital economy. Mishandling of data by a small number of companies should not brush the entire industry in the same colour.

Anonymization of data: The Draft Policy states that the interests of individuals are not separated from data even when it is anonymized. 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.

- Market dominance is subject matter of competition law. GoI has undertaken a review process. While this policy could incentivize development of infrastructure, market forces should be the determinants for competition.

  The proposed strategies restrict cross border data flows, access to data in India, and will make it difficult for all entities – Indian and non-Indian and fundamentally keep Indian and entities in India from reaping the benefits of a seamless digital economy.

  Restrictions on cross-border data flows would not address concerns about first mover advantage but would suppress the entire economy by impeding innovation, raising costs, cutting off access to the most advanced technologies and services.

- Imposing restrictions on cross border data flows will have a negative influence in the digital economy and will stand in the way of India becoming the AI, data capital and digital hub for the world. Data transfers should be allowed on the basis of a consent-based regime, ensuring compliance to the highest standards of privacy and security measures. Data is not valuable unless business models are developed around it and AI led insights gathered for augmenting human efforts. Not permitting cross-border data flows will restrict access by Indian entities to the best tools and data-sets from abroad and delay their development of world class business and technical models and solutions.

  We also recommend addressing these issues through the Personal Data Protection Bill, 2018 and not through an e-commerce policy.

- The policy focusses on introducing restrictions to cross border data flows and use of personal data. The focus on 'India' and for domestic growth drives the strategies, including restricting access to non-Indian entities. It further undermines the provisions of cross border data flows proposed in the Personal Data Protection Bill.

  The approach outlined in the policy introduces barriers to operation and serious restrictions on data flows, and are unlikely to even provide any of the benefits being sought- rather, they are more likely to have adverse impacts and can curtail use of new technologies in India. This will have a negative impact on the Indian IT sector. Today sectors like Retail, Banking, Automotive are leveraging advanced analytics tools to gain insight into their consumer behavior. These insights in turn are used to develop products and services tailored to their needs.

  Leading globally responsible companies in the sector will have "Data responsibility principles", Further, the unique insights derived from clients' data are their competitive advantage, and these companies will not share them without their agreement, unless clients agree to such use and will limit that use to the specific purposes clearly described in the agreement.

  Additionally, such companies employ industry-leading security practices to safeguard data. This includes use of encryption, access control methodologies, and proprietary consent management modules which allows them to restrict access to authorized users and to de-identify data in accordance with applicable permissions.

- B2B Data (other than personal and sensitive personal data) will not see any data flow restriction if shared under a commercial contract.

  While this is expected to simplify under certain conditions, reference to community data could introduce restrictions on data collected from IoT devices is a cause of concern.

  Procedures to secure and protect ALL data and ensure lawful collection and processing should be made robust, thereby taking away the need to debate what does and doesn't need to be restricted with adequate safeguards in place, then it should be possible to transfer data across borders to facilitate growth of the digital economy and derive the greatest benefit from the data for India and Indians.

  The suggested strategies related to restrictions in cross border data flows, deny access to non-Indians etc. neither serve to enhance privacy or offer better protection.

- Data responsibility principles of globally responsible companies respect data ownership as outlined in the policy. As per their practices, Clients are not required to relinquish rights to their data to have the benefits of their solutions and services.

  The unique insights derived from clients' data are their competitive advantage, and they will not share them without their agreement.

Their client agreements are transparent and the companies will not use client data unless the client agrees to such use and they will limit that use to the specific purposes clearly described in the agreement.

Such companies employ industry-leading security practices to safeguard data. These include, use of encryption, access control methodologies, and proprietary consent management modules which allow them to restrict access to authorized users and to de-identify data in accordance with applicable permissions.

The Personal Data Protection Bill is expected to lay down codes of practices and standards for consent, express consent. WE urge the Government to therefore let Data related issues be handled by MEITY under the data protection law and not introduce complexities by introducing more rigid policy provisions under the ecommerce policy. As mentioned above, the Data Protection Policy is being built on extensive multi-stakeholder inputs and eCommerce policy may like to leverage the existing work on Data for the purpose of this policy.

- The Policy raises several questions related to Community data, and questions rights of entities on such data of a particular group, and right of a company to exploit or monetize.

  It further questions the efficacy of anonymized data and raises questions on its ownership and need for restricting its use. Such a concept undermines the exemptions for anonymized data offered under legislations like GDPR that have been through rigorous consultation and evolution.

  It is important to evaluate the possible difficulties entities may encounter should there be a community ownership to data. For example, initiatives to develop insights into local agriculture produce, soil health and suggestions for better yields, can see huge delays due to compliance for community data and seeking consent from joint owners etc.

  The policy appears to be extremely sensitive to misuse of data, at the risk of disregarding the benefits that can accrue from analysis of data and leveraging it for AI and augmented decision making. Denying benefits from such technologies will be a set-back to Digital India aspirations. Policies protecting privacy and securing data wherever it is stored, processed or transferred would be helpful.

- The draft policy suggests protectionism measures for access to data, that extends to anonymized data. However, it would be helpful to have clarity on the definition of a domestic company.

  Strong mechanisms should be in place where defaulters should be penalized. This will ensure the seamless nature of the Internet is not fragmented, and India continues to benefit from the growth of the digital economy globally.

  Restrictions on data flows come with a cost: reduced innovation, loss of access to leading technologies and services, increased cost of services, less competitive industries across all sectors, reduced ability to apply AI for the benefit of the Indian economy.

India will benefit from sharing data and allowing the aggregation of large data sets that combine data from India with data from other countries. Some examples include research into cures for diseases, enhanced weather forecasting that can improve emergency preparedness and save lives, and detection and prevention of international financial fraud. AI and data analytics can provide better insights and greater value when larger data sets are available.

- The principles of personal data protection require informed consent, collection limitation, purpose limitation, storage limitation, as well as grounds for lawful processing. Any data that is collected and processes are governed by these principles. This is also outlined in the draft Personal data protection bill.

  Allowing Indian companies to have access to "huge trove of data", can in fact be in violation of the basic norms of privacy and data protection. It is a wrong assumption that by keeping the data in India, it can be easily accessed by Indian companies. This assumes that such data can be given freely, and without too many restrictions. This also ignores the technological reality that Indian companies can access this irrespective of location, if agreed with the data controller. Further, mere access to data, without entrepreneurial ideas will not lead to development of digital products.

  We therefore request that the policy should focus on enabling capabilities and capacities to collect and use data, support start-ups and small companies in their efforts to develop products, services and solutions by leveraging data, instead. This will also serve to assure individuals and citizens that their private data is not under threat.

- The policy forbids sharing of any sensitive data with business entities outside India, even with customer consent, including for third party processing. While the policy allows entities to use cloud facilities outside India, it strictly prohibits sharing for personal data with foreign entity, even if it is for processing. The policy further disallows any foreign entity from accessing sensitive data of Indians. There is no definition of what is sensitive data.

  The Draft Data Protection bill is already defining it after extensive consultations and references to global practices. It further undermines the globally recognized data sharing mechanisms, including the ones proposed in the Personal Data Protection Bill. There is a need for clarity on what qualifies as a domestic / Indian entity to judge full impact of such restrictions.

  Ensuring ethical and legal use of data is not decided by its location but rather on the processes and oversight mechanism that an entity has, as well as regulations in the country. We believe the intent of the policy should be to develop a process that will ensure proper use of data, in the interest of consumer privacy and protection.

  Merely making data access difficult neither guarantees data protection or innovation and digital products. However, such restrictions can be detrimental to India's digital India aspirations and impact the Indian IT industry and its competitiveness.

Further provision 1.2(d) recognizes that it is possible for the GoI to require access data to data stored outside of India. Therefore, it is not necessary to impose cross-border data flow restrictions to meet this government need.

- The Data Authority should define norms for community data and sharing of such data in larger public interest.

  This provision appears to be contradictory to the concept of community ownership and benefits accruing to community, as it seeks to share data with start-ups and firms, under conditions that Government will decide, taking away the rights of individuals on their own data.

  The policy intent and the provisions should be consistent with the Personal Data Protection Bill and individual rights to Privacy.

- The draft policy calls for a legal and technological framework to restrict the cross- border flow of data generated by Internet of Things (IoT) devices and users of certain digital services. But access to data is not determined by the physical location of the servers on which that data is stored, and preventing the cross-border flow of data would not achieve the objective of maintaining control over the "national asset." Rather, by raising barriers to IoT and platform companies, the draft policy would raise costs for firms, especially foreign firms, which are more likely to process and store data outside India. These firms likely will seek to pass those costs on to their Indian customers or clients – many of which are small enterprises. The likely ultimate effect of this provision would be to cause those companies to reduce investment in India, decreasing the amount of data they create and collect and eliminating domestic economic activity that could otherwise have been generated by that data. In addition, Indian data might be removed from global data sets that could otherwise have benefitted India and the world.

  The purpose of legal and Technological framework appears to be to introduce restrictions on data flows. It includes data collected by IoT devices as well, and suggests basis of sharing with domestic companies.

  This wide coverage of data will have a direct impact on the digital economy. Further, references to domestic companies implies a framework for granting preferential access to data.

  While it is not clear how domestic companies will be defined, but imposition of such policies will distort the business environment and can directly impact the growth of the digital economy in India. It can potentially impact FDI and investments in the country as well.

- The importance of accessing data and protecting in particular personal data: in fact, improving access to reliable data helps making design more innovative and increasing quality of products and services, which could be improved by:

  1. Making available public sources of information by putting those in structured and accessible databases;

2. Actively supporting the creation of reliable datasets in India which could be used by all AI developers, by start-ups and more broadly by industry to test automated solutions and benchmark the quality of their algorithms;

3. Fostering incentives for data sharing between public and private sector and among industry players.

To do all of the above, strict limitation to cross-border data flows would not be needed. In addition, promoting the free flow of data from and to India would reinforce the opportunity for India to create diverse datasets. Diversity reduces the risk of biases and ensure more accurate results, especially in sectors like healthcare.

While we acknowledge that governments may have a number of legitimate reasons to require the storing of a copy of the data within their country, we believe that defining those situations would not prevent policymakers from promoting cross border data transfers, especially if appropriate measures are adopted to protect data and the individuals it relates to (e.g. encryption, anonymization).

Preferential treatment of Digital Products created within India:

- Domestic alternatives: The Draft Policy seeks to develop domestic alternatives to cloud service and email and grant preferential treatment to digital products created within India. In today's globalized world, software and hardware development depend on globalized supply chains. Thus, it is unclear what constitutes a "domestic" alternative or an "Indian" digital product. A product could be developed by Indian engineers, or by India registered companies, or using Indian capital, or on the soil of India, or even by companies owned by Indian passport holders.

  India attracts significant global R&D efforts due to its light touch regulatory framework. Imposing protectionist restrictions may hamper such efforts and drive global businesses outside India – leading to a loss in consumer welfare.

  Domestic Standards: Harmonizing standards is a global initiative in order to ensure interoperability, global scale, upward and downward compatibility etc. If the Draft Policy seeks to create domestic standards that are isolated from global standards, then this will hamper global sales of Indian products and services.

  Mandatory Data Sharing: This is again a misplaced priority under the premise that it will ensure a level playing field for Indian enterprises. Mandatory sharing of data impacts proprietary rights of business entities and entrepreneurs. If the objective is to help small companies to innovate by making data easily available, Government which is the largest holder of citizen data, can start by sharing the data held by it.

  Law Enforcement Access to Data: It is very well appreciated that Government investigation and enforcement agencies may require access to data for ensuring National Security and Law & Order, and the industry must cooperate and collaborate. However, to enable that Government must consider a principal based approach to law enforcement access, with built-in safeguards to protect individuals' privacy, as well ensuring that there is a due legal process with appropriate judicial oversight over demand orders, and overall transparency in the process, etc. Confining

data to physical boundaries do not serve this purpose in the digital world, especially when nations have to fight cybercrime beyond national geographies and international borders.

- The policy seeks to support and strengthen the Preferential market access policy

  Product development leverages global competencies that maybe distributed across locations. Such policies can impact the product development efficiencies. Further, Preferential market access for technology products not only distorts the market, but also acts against consumer interest, by depriving them access to cutting edge technologies globally.

  Preferential treatment for domestic companies will shield those companies from competition and make their products uncompetitive in the global marketplace.

  The draft policy is expected to provide guidance and a blueprint for negotiations in multilateral and bilateral platforms.

  It appears that this proposal will lead to the government having the ability to demand source code, and then release it to a larger audience. Seeking disclosure of source code for ToT and development of application undermines the company's innovative solutions and IPR. Further licensing conditions for facilitating ToT could also undermine the open source licensing T&C.

  Source code disclosure would unnecessarily impede innovation, discourage investment in India, and cut off India from access to advanced technologies and services. Source code disclosure could cause companies to refuse to make their most advanced applications available in India so as not to put their valuable intellectual property at risk.

  Any circumstances where source code may be required should be the subject of bilateral discussions and negotiations and captured in contract.

Disclosure of Source Code & Algorithms:

- Access to source code and algorithms has been proposed in the interest of transparency.

  Transparency in AI and ethical AI are important issues. Globally responsible companies have been introducing disclosure norms and also investing in research to develop bias checking algorithms for example.

  A holistic approach by promoting research, development of tools and interdisciplinary collaborations to deal with concerns related to AI may be considered as alternatives to source code disclosure to give governments confidence in the software, such as AI fact sheets, software testing, review of development procedures and security safeguards, etc.

- Explicability is essential to increase trust in AI. Therefore, the aim should be to provide intelligible and meaningful explanations of AI-based decisions. Explainable AI should not be understood as disclosing source code or algorithms. Disclosing an algorithm would not be informative to users and would be a challenge for Intellectual Property Rights and security. In

some cases, disclosure could also facilitate abuse and undermine the algorithm. Therefore, explicability of an AI system should address how it has been trained and with what data, and the ability to explain how the AI system decision has been generated.

Industry is contributing to the creation of voluntary standards for algorithmic explanation for different AI implementations that will allow for discerning the logic of deep-learning decision making without the need for disclosure of trade secrets and IP.

- One of the pre-requisites of having a favorable business climate is to create, protect and respect Intellectual Property. Source code and algorithm escrow is an uninformed policy position. There are several questions that have not been addressed such as who will hold and secure the source code, who will indemnify the commercial entity in case there is a leak of the source code, how the updated source code will be provided to the Government given that there are constant product upgrades, and what kind of market failure or customer concern this is seeking to address. This kind of policy regime will stifle innovation and deter development of digital tools and disruptive AI solutions.

- When companies export software and other products to foreign markets, they need to be sure that they will not be forced to give up valuable proprietary information as a condition of market access. The draft policy articulates a range of bases upon which the Government of India would retain its right to mandate forced transfer of source code, algorithms, and other technology. In certain cases, governments may have legitimate regulatory reasons for requiring access to source code or algorithms, such as evaluating the safety and security of new technologies, or enforcing competition laws. But there is no legitimate reason to require transfer of such sensitive information as a precondition for importing or selling software and other products.

  In particular, requiring source code disclosure to facilitate technology transfer, as articulated in the draft policy, would de-incentivize investment in India and discourage foreign firms from serving the Indian market with their most up-to-date technology. Given India's comparative advantage in software development, this approach would appear to set a precedent highly detrimental to India's own long-term economic interests.

Duty Tariffs & Taxes/Customs Duty:

- The longstanding WTO moratorium on customs duties on electronic transmissions has been essential to the development of the global digital economy by preventing protectionism in an emerging engine of economic growth. Some of the greatest beneficiaries of the moratorium are artists and entrepreneurs who can export online without worrying about customs processes, and small businesses that can import the best software, duty free. The moratorium allows India's own businesses to export a wide range of digital products on a level playing field. For example, India's film and creative industries stand to lose a great deal if their products become subject to duties in foreign markets. What is more, imported digital products often complement rather than substitute for domestic digital products. For example, Indian app developers likely produce and sell their products using imported software. Imposing customs duties would raise the cost of that software for India's own artists and entrepreneurs.

  The draft policy raises concerns with respect to the moratorium's future implications for governmental revenue; India should also consider the likely economic costs of imposing

customs duties on electronic transmissions, which may outweigh any benefits. Furthermore, it is widely understood that the e-commerce moratorium does not preclude internal taxes or fees otherwise compliant with GATT Article III, allowing governments to collect revenue on digital transactions without creating new barriers to trade. Every WTO Member—including India—should be ready to make the moratorium permanent, and it is regrettable to see the draft policy taking a position to the contrary.

- Government should commit to refrain from imposing duty tariffs or taxes on cross-border data flows and digital products, so that all firms can compete on a global level playing field and all consumers have access to the best and most innovative digital technologies, services and products in order to avoid a digital divide.

Local Storage of Data:

- The draft policy identifies job creation as another rationale for creating barriers to cross-border data flow. However, requiring local storage of data does not create many jobs: data centre's do not employ large numbers of people or generate much local economic activity. Rather, data localization requirements often act as a drag on the local economy, raising costs and burdens for local firms that could otherwise capitalize on the economies of scale afforded by global cloud computing services. By forcing potentially inefficient investment in data storage, India might also direct resources away from other possible economic strengths, such as advanced analytics and software development.