IndusLaw Comments on the Draft National e-Commerce Policy:

The Draft National e-Commerce Policy ("**Policy**") has sought to address six broad issues of the e-commerce ecosystem: (i) data; (ii) infrastructure development; (iii) e-commerce marketplaces; (iv) regulatory issues; (v) stimulating domestic digital economy; and (vi) export promotion through e-commerce. In relation to each of these broad issues, the Policy has provided general principles to be considered as well as specific strategies to be adopted to achieve the stated goals. We have set out our general observations on the Policy, followed by specific comments in relation to some of the proposed strategies and changes.

Definition of E-commerce

There is no universally accepted definition of e-commerce. In this Policy, the terms 'e-commerce', 'electronic-commerce' and the 'digital economy' are used interchangeably, as the context requires. E-commerce includes buying, selling, marketing or distribution of (i) goods, including digital products and (ii) services; through electronic network.

IndusLaw Comment: In the context of digital economy, the Policy refers to search engines and social media platforms in many places. The inclusion of strategies or proposals for regulating search engines and social media platform within a policy for e-commerce suggests that it seeks to expand the commonly used definition of e-commerce in India.

The definition of e-commerce adopted by the Department of Industrial Policy and Promotion and Reserve Bank of India for the purpose of foreign investment in India is restricted to buying and selling of goods and services and is intended primarily to ensure that restrictions on retail trading in the physical space is also extended to electronic space. Given the inherent contradiction of the definition of e-commerce (which includes buying and selling of 'services') for the purpose of regulating marketplace of e-commerce with the exemption of sale of services through e-commerce from the marketplace of e-commerce as a sector, there is an industry view that the e-commerce definition, for the purpose of foreign investment in India, is limited to buying and selling of goods (and does not extend to services). This Policy could have thrown some light on this regulatory uncertainty. Rather than doing so, the Policy has attempted a conflation of digital economy (including social media platforms and search engines) with e-commerce, resulting in creating new restrictions on foreign investments in India. Revising definitions, without an amendment to the existing legal framework, may result in unnecessary regulatory uncertainty without any tangible benefit.

S. No.	Reference in the Policy	Proposal	IndusLaw Comment
I - DATA			
1.	1.1	A legal and technological framework to be created that can provide the basis for imposing restrictions on cross-border data flow from the following specified sources: a) Data collected by IoT devices installed in public space; and b) Data generated by users in India by various sources, including e-commerce platforms, social media, search engines etc. The legal and technological framework would also provide basis for sharing the data collected by IoT devices under (a) above with domestic entities for use in research and development for public policy purposes.	**Cross-border Data Transfer:** The intent of this proposal seems to be towards curbing cross border transfers of certain types of data/or data handled by certain types of organizations and ensuring that the data is stored within the country. The Policy provides the justification for this approach, by stating that in the absence of this approach, Indian business entities will not be in a position to have access to data generated within India, and as a consequence will not create high value digital products and would only be processing outsourced data. Further, another reason which the Policy anticipates is the increased spending on creating data infrastructure in the country, which would lead to more jobs and is economically beneficial. In our view, none of the above objectives will be effectively achieved by the proposed restrictive approach to cross border transfers and the effect on the industry will be contrary and disproportional. The underlying principle of an e-commerce policy has always been protecting the user, promoting trade and commerce for the benefit of the user and aiding innovation. This principle appears to have lost its shine in the Policy. In the first instance, access to information has little to do with the localization of information. Today most corporations handling large volumes of data may choose to store the data overseas, as a result of use of third-party cloud service providers, cost considerations, business objectives, etc., in accordance with the applicable data privacy law in India, but still have access to the data generated in India for the purpose of creating digital products. The Policy restricting the sharing of personal data only to entities in India, may restrict the ability of multi-national companies to transfer and process personal data across different

			jurisdictions and unnecessarily affect the ease and ability of doing business globally. The 'White Paper of the Committee of Experts on a Data Protection Framework in India' under the Chairmanship of Justice B. N. Srikrishna, had justified restricting cross border flow, for reasons such as (i) protection of the rights of data subject in the country; (ii) preventing foreign surveillance; and (iii) enabling easy access to law enforcement. These grounds were severely criticized by way of public comments to the Proposed Personal Data Protection Bill ("**Proposed Bill**"). Security of information does not have any nexus to where the information is stored, but rather on the steps adopted to protect the data. To this extent, requiring steps to be taken towards data security is more effective. In fact, it is common practice for organizations to address concerns around data security by storing data in multiple locations across the world to prevent data failure. Foreign surveillance of data stored abroad may be a general concern, but the Policy has failed to demonstrate how this would be so in relation to data generated from IoT devices or by users of e-commerce platforms, social media or search engines. In terms of access to law enforcement, mere storage of data in India does not enable easy access. The data could be subject to end to end encryption which cannot be accessed by others except for the user. Access to law enforcement should be addressed by strengthening mutual legal assistance treaties or executing 'executive agreements' as proposed under the Clarifying Lawful Overseas Use of Data Act of the United States or by increasing international cooperation, but not by restricting movement of data. Demanding data localization fails to address the high costs and technical feasibility of implementing the same. This is likely to disproportionately affect smaller organisations (including technology start-ups) in India, who cannot afford the additional cost especially in terms of data storage. This would ultimately affect the ability of these smaller organisations in India to participate in creating high value digital products in India, defeating the objective of the Policy. Even the Proposed Bill recognized this by allowing cross border transfers in

			certain circumstances such as: (i) when the transfer is made subject to approved standard contractual clauses or intra group schemes; or (ii) the authority has prescribed transfers to a particular country or sector or organization as permitted. In addition to the concerns of smaller organisations, the government of India must take into account consumer welfare and a policy which reduces quality of services availed by Indian consumers cannot per se be considered to be in the national interest. Such a protectionist approach may be worse than the reduced comparative quality of life experienced by the Indian middle class in the 1980s since the affect of higher cost and lower quality of services will hit the lower income groups hardest. **Sharing of Data by IoT devices:** The Policy also recommends that the data collected by IoT devices be shared with domestic entities for use in research and development for public policy purposes. The Policy refers to the data as "*data collected by IoT devices installed in public spaces like traffic signals or automated entry gates*". To the extent IoT devices installed in public spaces are restricted to devices which are fully funded by the government or installed to serve the government, there may be limited objections to data localization and the government dictating where data is stored. However, this will only increase the cost for the government since service providers will need additional local infrastructure to support localization. Unless storing the data in India is relevant for compelling national interest, this should be avoided since as discussed earlier, there is limited nexus between where data is stored and data security. The data collected by devices in public space should not include devices owned and operated by private players, which will be an unfair obligation on the private players to reveal proprietary information and personal information of their users. It is also not clear from the Policy whether this mandatory data sharing in relation to data collection by IoT devices is in relation to

			personal data or anonymized and community data. To the extent that the data sharing relates to personal data, providing for mandatory sharing of user data collected by IoT devices is in conflict with one of the objectives of the Policy and the Proposed Bill, i.e., to empower users/consumers to have control over the data they generate and own. The mandatory data sharing, whether of personal data or community data, with local entities also, in many ways, is anti-competitive and the lack of level-playing field may discourage foreign corporations from providing their cutting-edge technology products and solutions to India. This will create a vacuum, the brunt of which will need to be faced by the user mostly, by having to choose between products that may not be at par with the innovative products available elsewhere in the world. **Types of data:** Even assuming, cross border restrictions are to be implemented, the primary determination to be made is to understand the nature of data which is intended to be restricted. Here, perhaps the question should be – whether the derived and observed data[1] of a user should be allowed to be siloed with the entity creating/collating them? The answer to this question will need to be traced from the question who owns the data? Is it: i) the user? The user provides her data for a defined purpose only. If through deep learning or machine learning the entity collecting such information generates additional derived or observed data, can it be argued that the ownership of such data will continue with the user?, or (ii) can the entity which has invested the capital, technology, man-power and time to develop such artificial intelligence, and created intelligible

[1] Broadly, data can be categorized into three types: (x) collected data, i.e., information that fed into the system by the user directly or indirectly, (y) observed data, i.e., the data, patterns and information collated by observing the user's activities online, and (z) derived data, i.e. data derived from existing data points at various sources.

			data be the owner of such information? If the answer to this question is: i) 'user', then the right to decide on whether a user wishes for her derived and observed data[2] should be with the user. ii) corporation creating/collating the derived and observed data, then restriction could be based on mandatory sharing of derived and observed data of the user with other entities on the basis of some objective parameter, user's consent and/or the nature of the recipient entity. An overall restriction on cross border flow of data, which banishes foreign players from having access, or control over the data of an Indian user would be draconian and harsh, not to mention anti-competitive and anti-innovation. In most jurisdictions, data protection is seen from the angle of protecting the privacy and personal information of individuals. However, the Policy seems to suggest that even non-personal information, such as anonymized data, would be covered. There is no clear justification provided for inclusion of anonymised data, beyond merely stating that it "*will always have something of value for them*" (individuals). To the extent that anonymised data can still be used to identify an individual, in most jurisdictions, such data has been clearly included within the ambit of personal data/information. Anonymised data has also been kept out of the purview of the Proposed Bill and the General Data Protection Regulation in European Union ("**GDPR**"). We hence believe that there need not be any cross-border restrictions in relation to sharing anonymised data. The Policy also seeks to cover community data within its ambit (especially in the context of data derived from IoT devices in public

[2] We leave out collected data here, because this form of data has been extensively dealt with in the Proposed Bill.

			space). It states that "*data about a group of individuals and derivatives from it is thus the collective property of the group*". This would refer to data which is linked to group characteristics but not to any particular individual, that is, it would not be personal information. In the context of targeted advertising where group identities or commonalities are used, this categorization and protection of community data may be useful. However, the definition of community data, restrictions on its use, and the manner of enforcement will need to be carefully determined, especially since privacy of individuals are not directly affected in cases where such data is anonymised. Nevertheless, in our view, controlling only cross border transfer of such information has limited relevance to how the community data is used. In relation to data ownership, the Policy states that "*India and its citizens have a sovereign right to their data.*". It also states that this data should be accessible equitably by Indians but non-Indians do not have equal rights to access the data. The Policy also has references of a few illustrations of data sovereignty frameworks including that implemented for Maoris in New Zealand and indigenous people in Canada. Curiously, the Policy has sought to extend the principles applicable to indigenous communities which face problems with traditional knowledge protection, to all of India. If this is interpreted in a broad manner, any data pertaining to Indian individuals or communities or collected in India should be preferentially used for Indians companies (potentially without foreign investment). This would be unnecessarily prohibitive to operation of business in India, especially by multi-national companies. **Need for technical framework:** To the extent the data sought to be protected is restricted to personal data, the Proposed Bill already provides for protection in relation to personal data of individuals. In fact, the Proposed Bill already contains restrictions on cross border transfer and a strict data localization requirement for data designated as critical personal data. Any risk arising from the transfer of personal data, especially

			in relation to data privacy point of view and providing users control over their personal data, will be addressed by the Proposed Bill. There is no additional objective relevant to having a separate technical framework for data collected by e-commerce entities, search engines or social media platforms.
2.	1.2	A business entity that collects or processes any sensitive data in India and stores it abroad, shall be required to adhere to the following conditions: a) All such data stored abroad shall not be made available to other business entities outside India, for any purpose, even with the customer consent; b) All such data stored abroad shall not be made available to a third party, for any purpose, even if the customer consents to it; c) All such data stored abroad shall not be made available to a foreign government, without the prior permission of Indian authorities; d) A request from Indian authorities to have access to all such data stored abroad, shall be complied with immediately; e) Any violation of the conditions mentioned above shall face the prescribed consequences (to be formulated by the Government).	**Sharing with third parties:** A complete prohibition on sharing data abroad with other business entities or third parties is excessive, undermines the Proposed Bill and is contrary to global norms. It is interesting to note that transfer is prohibited even when the customer has consented to such transfer. This would mean that companies which use the services of a third party to provide services to users in India will not be able to do so. This creates a requirement on companies storing information abroad to process it completely in-house, which would be impractical and prohibitively expensive in many cases. Further, such companies will not be able to leverage the cost-effective global cloud platforms that draw upon economies of scale, as they expand their operations or enter into a new market. To the extent the user is made aware of all the entities to whom the data is transferred, and has consented to such transfer, the transfer should be allowed. This approach is consistent with the global best practices. Any approach that allows or restricts transfer of personal data, in a way that negates or overrides user consent, will amount to a violation of the individual's fundamental right to privacy. Alternatively, a necessity-based provision may be used where data stored abroad can be transferred to other third party entities if the transfer is necessary for the performance of the contract between the customer and the company collecting data from the customer and storing the data abroad. This would ensure that the user data is not misused. If it is deemed necessary to prevent certain entities or categories of entities from receiving any data for security reasons, then the authority may consider creating such a list.

			Sharing with foreign government: The prior permission of Indian authorities before information stored abroad is made available to a foreign government may prove to be a challenge for companies situated abroad. A conflict of law question may also arise if another country also asserts jurisdiction over the data stored by the Indian company and demands access to data. Refusal to entertain lawful (*in accordance with applicable laws*) requests made by foreign government may expose the Indian companies to the risk of violating the applicable law. Alternatively, the suggested Clause 1.2(c) may be implemented if the Indian government will concede to a similar framework by foreign governments where data collected overseas by Indian companies and stored in India can be accessed by the Indian government only after obtaining approval from the relevant foreign government. This may be mutually discussed between governments in a manner which does not indirectly result in companies not being able to operate in certain jurisdictions or operating in a manner that violates the applicable law.
3.	1.3	Restrictions on cross-border flows of data shall not apply to the following: a) Data that is not collected in India; b) B2B data sent to India as part of a commercial contract between a business entity located outside India and an Indian business entity; c) Software and cloud computing services involving technology-related data flows, which have no personal or community implications; and d) MNCs moving data across borders, which is largely internal to the company and its ecosystem, and does not contain data that has been generated	As we have stated in our comments in Sl. No. 1, there is limited justification for creating additional restrictions on cross border flows of data, especially in relation to the data that is being sought to be covered (e-commerce, search engines, social media etc.). The Proposed Bill already addresses any data privacy concerns arising from cross border transfers of personal information by ensuring that such transfers take place upon the satisfaction of prescribed conditions. Even if such restrictions on cross border transfers are to be implemented, the exceptions provided are extremely narrow. The exceptions provided would not allow companies providing services to Indian customers, both incorporated in India and abroad, from making use of any service providers situated abroad for processing of data. For instance, a mobile app developer in India relying on authentication services provided by foreign service provider would

		by users in India from various sources, including e-commerce platforms, social media activities, search engines etc.	not be able to do so anymore and would need to develop the capability in house or find some other service provider in India. At the minimum, exceptions will need to cover services obtained by companies situated in India (from third parties situated abroad) which is utilized for the services provided by the Indian company to the end user. For instance, an e-commerce entity may choose to store all information, including personal data on the cloud, for added security measures or ease of doing business, which will no longer be permitted. The preferred framework for cross border transfers should be as provided in the Proposed Bill where cross border transfers are permitted on the basis of adequacy decision by the authority or on the basis of approved standard clauses or intra group schemes. This would allow companies more flexibility in transfers while also ensuring data privacy and security.
4.	1.4	Suitable framework will be developed for sharing of community data that serves larger public interest (subject to addressing privacy-related issues) with start-ups and firms. The larger public interest or public good is an evolving concept. The implementation of this shall be undertaken by a 'data authority' to be established for this purpose.	The term 'community data' has not been defined or explained in the Policy. To the extent that community data consists of personal data of users, mandatory data sharing may infringe upon the individual right to privacy. As we have noted above (*Public Space and Data Sharing)*, the mandatory data sharing requirement whether of personal data or community data, with local entities also, in many ways, is anti-competitive and the lack of level-playing field may discourage foreign corporations from providing their cutting-edge technology products and solutions to India. Even when community data is being shared, it is important to understand the manner in which it is to be shared. If only the raw data is required to be shared without the analysis or analytical capability, then it may not be of much utility. The critical requirement of big data is the analytical capabilities, without which the data is rendered useless. Further, if the intention is to treat companies handling big data as providing utilities such as electricity, then frameworks for licensing and pricing may need to be put in place, similar to how it is done for other utilities such as electricity.

			In terms of community data collected or processed by private entities, the impact of mandatory sharing would have a detrimental effect on the private entities. Mandatory sharing of community data removes the incentive for any entity to collect the data in the first place since it will result in a free riding problem.
III - E-COMMERCE MARKETPLACES			
5.	3.4	All ecommerce sites/apps available for download in India must have a registered business entity in India as the importer on record or as the entity through which all sales in India are transacted. This is important for ensuring compliance with extant laws and regulations for preventing deceptive and fraudulent practices, protection of privacy, safety and security.	The provision requires the existence of a mandatory business entity in India as the importer on record. This necessarily means that customers currently having the option to purchase products from global apps/websites will not be able to do so, unless the entity operating the online platform has a physical entity in India. This measure shall greatly impact the convenience of Indian customers and may restrict them from utilizing a legitimate channel of import. On a related note, the provision does not seem to make a distinction between goods and services. The Policy defines e-commerce as including buying, selling, marketing or distribution of (i) goods, including digital products and (ii) services; through electronic network. Hence, in light of the broad definition of e-commerce, accessing a website/app available for download in India, even if the website is purely for information purposes and does not facilitate cross-border sales, may be viewed as import of services, thus requiring the existence of a local business entity. This is likely to have disproportionate impact for businesses and consumers in India since many offshore entities may prefer to not offer their websites/apps in India for and may accordingly block access in India.
6.	3.5	All e-Commerce sites/apps available to Indian consumers (displaying prices in INR) must have MRPs on all packaged products, physical products	This requirement should not be extended to e-commerce marketplaces (especially with foreign investment) which are not permitted to hold inventory or sell their own products on the

		and invoices. Department of Consumer Affairs would evaluate violations and decide corrective actions for such sites/apps.	platform. The requirement under the Legal Metrology Act, 2000 and the accompanying rules is to display the price of the product on the platform. This is a requirement the e-commerce marketplace will be in a position to satisfy. However, the e-commerce marketplace will not be in a position to verify whether the label of the product comply with the requirement to display MRP. This fact has also been acknowledged by the Legal Metrology Act and associated rules, which provides that the responsibility for compliance should be on the seller and not the e-commerce marketplace platform. Hence, the e-commerce marketplace platform cannot be held liable for any violations, as contemplated under the Policy. To the extent it pertains to e-commerce platforms selling their own goods, then this requirement is already present under the Legal Metrology Act, 2000.
7.	3.11	Trade mark (TM) owners shall be given the option to register themselves with e-commerce platforms. Whenever a trade-marked product is uploaded for sale on the platform, the platform shall notify the respective TM owner. This facility shall be put in place by platforms and made available for interested TM owners.	The requirement to notify the TM owner regarding any of their trade-marked product offered for sale creates a positive obligation on e-commerce entities to individually verify all the products offered for sale on the platform. In MySpace Inc. v Super Cassettes Industries Ltd., the Delhi High Court recognized the impracticality of asking an intermediary to search through infringing content based on a general list of intellectual property owned by the owners of the intellectual property. It held that the owners would be required to provide specific details as well as the location of infringing content before it can be taken down. In our view, trademark owners have sufficient protection by being in a position to request for take down. The principles around takedown of infringing content and the e-commerce platform's related obligations have been discussed in several judicial precedents. The process for takedown requests may be simplified and should require cooperation from the intermediary. However, it would be excessive to require the e-commerce platform to go through the entire list of the products listed and notify the registered TM owners. It is also to be noted that the proposed Information Technology [Intermediary Guidelines (Amendment) Rules, 2018

			("**Intermediary Guidelines Proposed Amendment**") already contemplates use of automated technology based tools to identify 'unlawful' information or content, which may potentially extend to trademarks. This measure was severely criticized as legislative overreach. The proposal in the Policy goes beyond what was proposed in the Intermediary Guidelines Proposed Amendment since it requires the e-commerce platform to play an active role and potentially manually identify all trade-marked products sold online, regardless of whether the same is unlawful or not. This may also be a practical challenge in cases where there are multiple TM owners/licensees involved. On a separate note, this proposal in the Policy is also contrary to the principle of national exhaustion, recognised in the case of the case of Samsung Electronics Company Ltd. & Anr. v. G. Choudhary and Another[3], where the court held that ***once genuine goods are released into commerce anywhere by or with the proprietor's consent, all associated Indian trademark rights are exhausted***. *Such consent may be express or implied, direct or indirect. The underlying rationale* ***for liberal exhaustion is that trademarks are deemed to connote trade origin and not control.****.."* *"Section 30 of the New Act (Trademarks Act, 1999) provides that where* ***the goods bearing a registered trade mark are lawfully acquired, the further sale or other dealings in such goods by the purchaser or by a person claiming to represent him is not considered an infringement if the goods have been put on the market under such mark by the proprietor or with his consent****.".* The principle of national or international exhaustion as discussed hereunder stipulates that once a product has been sold for the first time in the domestic market with the consent of the proprietor of the trademark, the proprietor ceases to or exhausts the control over any

[3] CS (Os) No. 1602 of 2006; Vikramajit Sen; 2006 Indlaw DEL 1386, 2007 (136) DLT 605, 2006 (33) PTC 425

			further sale of the same product. The Supreme Court, in appeal, is yet to decide whether the Trademarks Act, 1999 also extends to international exhaustion of trademarks.
8.	3.12 and 3.13	In case TM owners so desire, e-commerce platforms shall not list/ offer for sale, any of the owners' products without prior concurrence. However, in case TM owners choose to opt for this, they would have to undertake to respond to platforms within a certain time limit. In case of specified high value (luxury) goods, cosmetics or goods having impact on public health, marketplaces will be required to seek TM owner's authorization (that is, authorized/distributor/reseller agreement) before listing the product.	Please refer to our comment above. This would require the e-commerce platforms to keep track of all the products listed and would also increase the time it takes for a seller to list the product on the platform. The trademarks owners already have mechanisms under law to protect their trademarks and prevent sellers from undertaking sales without authorization. This would also affect the sellers selling the products online as opposed to those selling the same products offline and adversely impact competition. Further, strict compliance with this provision may result in violation of the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Intermediary Guidelines) Rules, 2011 ("**Intermediary Guidelines**"). The IT Act and the Intermediary Guidelines states that the intermediary shall not select or modify the information contained in the transmission. An exception is provided in relation to removal of access to the information after receiving actual knowledge of any intellectual property infringement or of a court ordering takedown of unlawful content. In this instance where the e-commerce platform is expected to remove access until approved by the TM owner, particularly in cases where the e-commerce platform is simply an intermediary/marketplace, it may amount to a violation of the IT Act and Intermediary Guidelines, which will result in the e-commerce platform losing the safe habour protection granted to intermediaries.
9.	3.14	In case a complaint is received about a product being fake/counterfeit, the same shall be conveyed within 12 hours to the owner of the TM. If the owner of a TM informs the platform about the product being sold on its platform to be counterfeit, it shall notify the seller and if the seller is unable to provide	The requirement should not be on the platform to assess the evidence provided by the seller and verify whether the product is genuine. This would not only increase the compliance costs for the platform but may also prejudicially affect the TM owners due to delays in removing the product. The market practice is for intermediaries to comply with take down requests from valid

		evidence that the product is genuine, it shall take down its listing and notify the TM owner of the same as per the provisions of law	owners of intellectual property without verifying the validity of the request. This was also implicitly recognized in MySpace Inc. v Super Cassettes Industries Ltd where the Delhi High Court noted that "*Under Section 79(3) read with Rule 3(4) of the Rules posit an intermediary on receiving "actual knowledge" or upon obtaining knowledge from the affected person in writing or through email to act within 36 hours of receiving such information disable access to such information. If copyright owners, such as SCIL inform MySpace specifically about infringing works and despite such notice it does not take down the content, then alone is safe harbor denied.*". This suggests that upon receiving actual knowledge (which refers to information of specific works and location of infringing content), the intermediary has to remove access to the content without examining the validity of the claim made in the notice.
10.	3.16	Since counterfeiting is a major concern, in case a customer makes a complaint to that effect, marketplaces would have liability to return the amount paid by the customer. In addition, the marketplaces shall cease to host the counterfeited product on their platform, thereby taking down every information related to the product.	This would go against the principle of protection of intermediaries subject to them complying with due diligence requirements. On the one hand, the Policy has attempted to increase the due diligence requirement of intermediaries which results in additional protection to owners of intellectual property. The basic premise of due diligence requirements is that the intermediary would not be liable for any of the specified violations (such as intellectual property infringements) on the electronic platform if the intermediary complies with the due diligence requirements. Therefore, increase in due diligence requirements should increase the protection provided to intermediaries against liability. However, the Policy has not only increased the due diligence requirements, but it has also affixed the liability on the intermediaries for which violations which occur despite satisfying the due diligence requirements. This approach is contrary to safe habour principles and should be avoided.
11.	3.17	Marketplaces should provide for creation of financial disincentives for sellers if found to be selling counterfeit products.	While we agree in principle with this proposal, the onus of determining counterfeit products should not be on the marketplace. At the same time, if the marketplace were to impose disincentives for sellers each time any customer of such seller makes a complaint against the seller for selling counterfeit products, this may give

			scope for misuse of the provision. It is hence important that the principles be laid down for implementing the financial disincentives against a seller. Further, financial disincentives can be seen as influencing the price of the products and not maintaining a level playing field, which entities with FDI are not allowed to do. Therefore, it should be clarified that as long as the marketplace follows the provided principles, financial disincentives will not be contrary to the requirement to provide a level playing field and to not directly or indirectly influence the price of the products.
12.	3.18	Intermediaries shall put in place measures to prevent online dissemination of pirated content.	It is not clear what additional measures the intermediaries are required to implement beyond those prescribed under the Intermediary Guidelines. The Intermediary Guidelines Proposed Amendment requires intermediaries to deploy technology based automated tools to proactively identify and remove unlawful content. This was uniformly criticized by almost all the stakeholders in their comments to the proposed amendment. If a similar requirement is to extent to pirated content, the same objections continue to hold good. The primary concern is that if failing to filter a particular content could endanger a service and its legal defences, then intermediaries cannot take a fair approach to content removals. This may result in the intermediary adopting a 'better safe than sorry' approach and may arbitrarily, excessively and disproportionately pre-censor information and content, having a detrimental effect on an individual's right to free speech. Then, an intermediary is often not in a position to identify or determine whether content is pirated, which is the prima facie role of the Courts and not of an intermediary. The provision seeks to shift the onus and duty of the State to private party and is against the Shreya Singhal judgment. Additionally, developing and implementing mechanisms to prescreen content is an extremely complex engineering task and can be very onerous to implement even by established intermediaries. For startups and relatively smaller intermediaries, it is an extremely high burden.

13.	3.23 and 3.24	Publication/display of phone number and email address for consumer grievances is mandatory for all ecommerce sites and applications where purchase and sale of products is taking place. A system of acknowledgment of consumer complaints to be put in place as well as clear cut timelines for their disposal.	In relation to e-commerce marketplace entities (including those having foreign investment), customer satisfaction is the obligation of the sellers on the platform and not the marketplace platform. While some marketplaces typically provide customer support services on behalf of the sellers, it is not a mandatory requirement. This requirement seems to shift the onus of addressing consumer complaints from the seller to the marketplace, which the marketplace may not always be in a position to do.
14.	(A) FDI	The FDI Policy in e-commerce has been developed in order to ensure that the marketplace provides a level playing field to all participants, while ensuring that distortionary effects, either through means of price control, inventory or vendor control does not happen. A situation of capital dumping is to be strongly discouraged.	Capital dumping should be certainly discouraged. Inherent nature of the market is to create monopolies. The best way to tackle this situation is through competition law. It would be hard to legislate against capital dumping, because the legal regime is to liberalize FDI and restricting investments through law would be considered protectionist and contrary to business-friendly policies.
IV - REGULATORY ISSUES			
15.	4.6	One area where this is manifested is the high rates charged for advertising by social media platforms and search engines. Traditional logic states that this should purely be a market driven activity. However, the presence of network implies that a few social media platforms and search engines virtually control access to potential consumers. This puts them in a position to charge monopoly prices also make it very expensive for new firms, small enterprises and start-ups to reach consumers. These firms do not have deep pockets. To reach the market (leave aside finding and maintaining their position there) they would have to allocate an excessively high proportion of their budget and working capital to advertising. juxtapose this with the high rates of capital. Thus, high advertising charges become a	Regulating the manner in which search engines or social media platforms decide to price advertising charges should be done in a cautious manner. Companies invest capital and resources in building innovative advertising tools. To control pricing of advertising tools would be an attempt to control the business models of digital advertising platforms. Pricing controls take the incentive away from digital platforms to further improve their advertising platforms and offering the various advertising tools they offer to the advertisers. While there may be network effects in play, any person wanting to advertise their product has multiple avenues, both online and offline, to advertise their products. Even taking online advertising as the relevant market, while a few companies may have a large proportion of the market in aggregate, it is to be recognized that a single company has not monopolized the market. The same

		barrier to entry. Advertising charges in e-commerce must be regulated, especially for small enterprises and start-ups.	principles which are followed by the Competition Commission in determining abuse of dominant position should be taken as the standard to determine if advertising charges are priced to the detriment of small enterprises or startups. However, if any regulation is considered necessary, the following points are to be noted: (i) The advertising charges should not be capped and should be left to market forces; (ii) The principle of fair and non-discriminatory pricing can be adopted as the standard. However, the principle should be interpreted in a manner where the social media platforms or search engines are required to treat similarly placed persons and products similarly, but not to provide the same charges to all persons or products. The regulation should also be implemented in a uniform manner, and not in a way that only focuses on e-commerce. This should be through the framework of Competition Act, 2002 to ensure regulatory consistency in addressing competition issues in India. In this context, it is to be noted that the Competition Act, 2002 does not prevent taking advantage of superior bargaining position or being a dominant position in terms of market share, unlike a few other jurisdictions where this is controlled. Any advantage received due to network effects need not be seen as abuse of dominant position but rather taking advantage of superior bargaining position. Therefore, if a shift in standard of competition law is sought, an elaborate consultative process should be undertaken rather than ad hoc implementation for e-commerce sector. One factor to be accounted for is that differential pricing based on reach or target audience is expected in any advertising. For instance, a television channel is permitted to charge different rates for advertising based on its TRPs. A conclusion of unfair pricing against smaller firms drawn merely on price difference without looking at underlying reason would be counterproductive to a market framework.

16.	4.7	The network effect must also be kept in mind while analyzing mergers and acquisitions. World over, the experience has been that e-commerce players like social media platforms have taken over potential competitors early. This prevents the emergence of the threats to market position later on. As discussed elsewhere in this document, the presence of network effect implies that it is virtually impossible for 'second-movers' to enter the market.	The analysis of network effect and its potentially negative link to maintaining a competitive market falls within the ambit of Competition Act, 2002 ("**Competition Act**"). The Competition Act only looks into certain types of combinations which are significant and are likely to have an appreciable adverse effect on competition in the relevant market. This is currently determined primarily on the basis of assets and turnover, with specific exemption for combinations which fall below a *de minis threshold*. In the context of technology companies who handle large amounts of data other factors such as transaction value may need to be considered if necessary. However, these changes should be implemented by way of an amendment to the competition law framework, after following an appropriate process. However, it is also to be noted that for a lot of start ups and promoters, this is the preferred exit option. This incentive may be removed if acquisitions are excessively regulated.
17.	4.8	Data effect and the network effect are the reasons why selling at a loss has emerged as 'sustainable' for enterprises. Leveling of the playing field, must therefore be seen from a data-lens. These are aspects which the anti-trust regime must take into account, to meet the challenges of regulation in the arena of e-commerce.	The suggestions seem to stem from the fact that bigger companies seem to engage in low pricing for excessive period of time to drive competition out of place. The classic predatory pricing concern is that the prices would eventually be increased once the competition is driven out of the market. However, the experience with e-commerce is that prices have remained low even in the long run. Under the existing framework of competition law where consumer welfare (as determined by prices) is prioritized, this effect seems beneficial. Nevertheless, as some competition law literature has suggested, consumer welfare based on price alone as the objective ignores the architecture of modern power where dominant e-commerce entities serve as critical intermediaries integrating across business lines. Alternative objectives can be explored within the competition framework for to protect markets and not merely consumers.
18.	4.10	In continuation, it is also important for the Government to reserve its right to seek disclosure of source code and algorithms. There will be a greater	The Government reserving the right to seek disclosure of source code or algorithms could have the unintended consequence of foreign companies choosing not to provide their services in the

		reliance on AI in decision making in future where parts of the process will become 'AI-fied'. Decisions will need to be explained. There is a need to strike a balance between commercial interests and consumer protection issues, as well as issues of larger public concern, like preventing racial profiling and maintaining constitutionally mandated rights, such as the right to equality.	Indian market. Source codes and algorithms are proprietary information or trade secrets which are a result of investment by the entity on research and development. Asking an entity to reveal the same and potentially transferring it to local competitors would result in loss of investment in research and development for the entity creating the source code or algorithm. The intent of the proposal appears to be to create a level playing field and a competitive market. However, to the extent of consumer protection, there are other mechanisms under the existing laws to ensure that consumers are provided a fair deal. For instance, the FDI Policy and recent Press Notes from DIPP on e-commerce ensures that consumers are provided treated in a fair and non-discriminatory manner. Compelling an e-commerce platform to compulsorily share their proprietary information and to lose their competitive advantage cannot be a solution. The possibility of algorithmic decision making resulting in biased decisions contrary to constitutional rights is an emerging concern in light of the proliferation of big data and machine learning. However, addressing this problem should be made on the basis of the results produced by the algorithm rather than by accessing and evaluating the underlying source code. The government may also ask the entity to provide information about the basic logic involved (as is required under the GDPR) in the decision making. For instance, the GDPR gives the data subject (individual to whom the personal data pertains to) the right not to be subject to decision based solely on automated processing which produced legal effects or affects the data subject, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. In any case, GDPR also provides that such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. This will address the issue without having to require the company to reveal the source code or logic.

19.	4.11	With e-commerce and the digital economy becoming a part of daily life of more and more Indians, unique law and order challenges are also emerging. Privacy is an important aspect and all possible efforts must be made to ensure it. However, law and order in society is something that we cannot live without. The Government must stand up to the challenge. Access to data for purposes of maintaining and ensuring law and order cannot be over emphasized.	The use of the words 'law and order' is vague and could potentially have a very wide ambit to collect data from intermediaries. This should be restricted to interests such as the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or concerning security of the State or cyber security, as contemplated in the Intermediary Guidelines Proposed Amendment. Allowing access to data for broad purpose such as 'law and order' could result in a surveillance state. Further, access to data should be subject to lawful order to avoid misuse of the power. The Proposal appears to provide the Government the right to: a. fish for information under the broader scope of maintaining law and order, thereby exposing the private information of citizens to scrutiny; and b. draw on the technology expertise of the e-commerce platform to help investigate a matter. The nature and extent of the assistance that can be requested from an e-commerce platform is not clear.
20.	4.13	In the presence of network effects which create barriers to entry, small firms and start-ups attempting to enter the digital sector can be given 'infant-industry' status. The benefits of an 'infant industry' status could be accorded to such firms and start-ups and access to data could be at the centre of this approach.	There is further clarity required on the criteria for categorization of 'infant industry'. The benefits provided should be designed in a manner that does not affect the level playing field. As discussed earlier, access to proprietary and user data of existing companies is not a reasonable benefit to be provided since it takes away the incentive for any entrepreneur to continue innovating.
21.	4.15	The atypical nature of an e-commerce transaction necessitates a consumer protection framework specific to this sector.	The Consumer Protection Bill, 2018 which was recently passed by the Lok Sabha already recognizes this aspect and now specifically provides for protection of consumers from unfair trade practices in e-commerce. There is hence no need for this to be a part of the Policy.
22.	I – Exemption	Online platforms and social media have become important tools to enhance outreach, mobilize social	The compliance requirements applicable to an intermediary are already provided in the Intermediary Guidelines and are the

	from content liability	welfare causes, promote trade, spread ideas and build business relationships. Internet penetration, coupled with user traffic, has brought these platforms and social media almost to every household in the country. With a growing importance of these entities, their social responsibilities also increases. Due to the fact that traders, merchants, individual users, organizations, associations are all dependent on them, the authenticity of content posted on their websites cannot be compromised. In this regard, it is important to emphasize on responsibility and liability of these platforms and social media to ensure genuineness of any information posted on their websites.	subject-matter of the Intermediary Guidelines Proposed Amendment. The obligation on social media and other platforms to ensure genuineness of information posted on social media is not only impractical, it could also potentially result in chilling effect on the freedom of speech. Further, the capability of social media platforms to verify the genuineness of information is doubtful. It may result in the social media platform adopting a low risk approach and deleting all information which is potentially contentious. Further, the suggested proposal in the Policy may put the e-commerce platform at risk of losing its safe harbour exemption under the Intermediary Guidelines.