March 29, 2019

Comments of the Computer & Communications Industry Association on
Draft National e-Commerce Policy: India's Data for India's Development

The Computer & Communications Industry Association ("CCIA") respectfully submits these comments regarding the Department for Promotion of Industry and Internal Trade ("the Department") consultation on the Draft National e-Commerce policy ("the Draft Policy"). CCIA appreciates the opportunity to provide its views on the proposed e-commerce strategy in India, and raise concerns about the strategy's projected impact on the growth of India's digital economy and implications for Internet services around the world.

CCIA is an international, nonprofit association representing a broad cross section of large, medium, and small companies in the high technology products and services sectors, including Internet products and services, electronic commerce, computer hardware and software, and telecommunications.[1] For over 40 years, CCIA has advocated for promoting innovation and preserving full, fair, and open competition.

As an emerging force in the global digital economy, a strategy that will further enable innovation in India is critical and India's commitment to studying these issues is welcomed. The Indian Government has set ambitious goals for the country's digital future. This is notable with India's improved ranking in the World Bank's *Ease of Doing Business* report for the second consecutive year.[2]

However, the Draft Policy presents a number of concerns from a trade and market access perspective, and proposes strategies that are unlikely to accomplish the stated goals of the Government of India to facilitate a competitive and vibrant Indian digital economy. CCIA's comments outline concerns with the Draft Policy's lack of clarity with respect to existing or pending legislation, as well as inaccurate representations of market dynamics within the global digital economy.

I. General Comments on the Draft National e-Commerce Policy

CCIA's comments outline specific concerns with strategies proposed in the following sections on trade restrictions, data, competition, intermediary liability, and taxation. However, CCIA has general concerns with the Draft Policy's intended operation in light of existing laws governing digital services in India.

A. Scope of the Draft Policy

Broadly, the Draft Policy lacks clarity regarding other laws, court decisions, and pending Digital India proposals, with which it often conflicts. This includes definitional concerns. For example,

[1] A list of CCIA members is available at https://www.ccianet.org/members.

[2] World Bank Group, *Doing Business 2019: Training For Reform* (2019), *available at* http://www.worldbank.org/content/dam/doingBusiness/media/Annual-Reports/English/DB2019-report_web-version.pdf.

'data' is referred to broadly, and the Draft Policy does not delineate between 'sensitive' and 'critical' personal data as is the case in the Personal Data Protection Bill, 2018. Further, it is not clear whether the Draft Policy seeks to treat 'e-commerce platform' or 'website' differently from their current classification as an 'intermediary' defined under the Information Technology Act, 2000 ("IT Act").

Further, there seems to be a lack of clarity with respect to what services the Draft Policy intends to target, and as a result, several entities that provide services not traditionally understood as 'e-commerce' but deal with large volumes of data will be impacted. 'E-commerce' is merely a subset of the entire digital economy, and should not be an interchangeable term for *all* digital services. For example, cloud service providers are a significant component of the digital ecosystem, but cannot be considered operators of e-commerce platforms as they primarily provide infrastructure services. Services that deal with large volumes of data will be impacted by the Draft Policy's stated position on data ownership, data localization, and data transfer norms. Conflating e-commerce with the entire digital ecosystem will lead to regulatory uncertainty and decrease investor confidence. As the entire world economy becomes increasingly reliant on digital services, regulators should be careful not to generalize diverse business models and services. To avoid any confusion, 'e-commerce' should be narrowly defined.

B. Nature of 'Data'

Within the document itself there are conflicting philosophies presented regarding the nature of data. For example, the document declares that data is an individual right and that India is pursuing a national strategy that protects this right. However, it also refers to data as a collective resource. It further suggests strategies that would mandate sharing of 'community data', which appears to be in tension with the stated importance of protecting personal privacy.

Defining all data as a "national asset" would grant the government unbridled rights over the control and alienation of data. This is in conflict with the Supreme Court's decision in *Puttaswany vs. Union of India*, where the court held that the right to exercise control over the dissemination of one's own data is safeguarded under the fundamental right of privacy. To avoid conflict with existing law, the Department should not classify data as a national asset, there should be no undue restriction on consent-based data processing and transfer, and what constitutes 'personal' versus 'community' data should be clearly delineated.

C. Overlapping Regulatory Regimes

In many cases, the proposed strategies conflict with existing legislation and precedent. It is not clear whether the government intends to override existing rules, or create additional obligations that could introduce conflicting responsibilities for digital services. Industry stakeholders cannot provide comprehensive, meaningful feedback without understanding how policymakers plan to resolve inconsistencies. As the draft contemplates many new approaches to data regulation and privacy policy, the Department should explain inconsistencies with the Personal Data Protection Bill, 2018. Clarification is also welcomed regarding proposed strategies' intersection with the Consumer Protection Bill 2018, the Information Technology Act, and India's new Foreign Direct Investment policy on e-commerce, among others.

Instead of treating issues pertaining to data privacy, control and ownership, and transfer to other jurisdictions through a parallel process envisioned by the Draft Policy, CCIA recommends that these issues be covered by the Personal Data Protection Bill. Likewise, payment-related issues should be under the purview of the Reserve Bank of India, which has already issued various regulations facilitating e-commerce payments including the Online Payment Gateway Service Providers Schemes. This would avoid creating conflicting or duplicative legal frameworks.

As the Department moves forward on any of the items raised in the Draft Policy, CCIA strongly encourages that additional guidance be provided to resolve these matters. CCIA also encourages further joint collaboration across Indian government authorities to ensure that there are not conflicting rules put in place and that all policy is justified by comprehensive analysis.

II. Disruptions Posed by the Draft Policy to Global Trade Flows and Innovation in India

The Internet is now an integral component in both goods and services. The value of global e-commerce markets reached $27.7 trillion USD in 2016, up from $19.3 trillion USD in 2012.[3] India has an increasingly vibrant e-commerce market, illustrated by the high value of digital exports and imports.[4]

However, the Draft Policy presents a number of strategies that threaten this market and pose market access barriers. The Department should reconsider proposals to further restrict data transfers, introducing new localization mandates that will do little to strengthen security, and not pursue strategies that undermine confidence in global trade.

A. Restrictions on Data Flows and New Localization Mandates

The Draft Policy's observation that "by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country" is contrary to global consensus and threatens the future of trade in India. Localization mandates should *not* be used as a trade development tool as they are ineffective to digital growth, and will inhibit the development of the local digital economy.

Cross-border data flows are necessary to the continued growth of the global e-commerce market. Firms of all sizes use data and moving data across borders is essential for day-to-day operations and communication across a variety of industry sectors. The OECD notes that cross-border data flows have also enabled the creation of "micro-multinational" micro, small and medium enterprises ("MSMEs") which are "born global and constantly connected."[5]

[3] WORLD TRADE ORGANIZATION, *World Trade Statistical Review 2018* (2018), *available at* https://www.wto.org/english/res_e/statis_e/wts2018_e/wts2018_e.pdf, at 21.

[4] *Id*. at 166.

[5] OECD, *Trade and Cross-Border Data Flows* (2018), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)19/FINAL&docLanguage=En.

In an increasingly connected world, data flows cannot be expected to remain confined within national borders. Data localization risks stifling competition, innovation, and trade. This does not provide better services for consumers, and can weaken data security. Policies should instead aim to facilitate frameworks that take into account the technological requirements of these services.

The Draft Policy's proposal to restrict cross-border data transfers for Internet of Things ("IOT") and machine-to-machine ("M2M") platforms will hinder growth of the increasingly valuable IOT industry and deny users technological benefits of these new services. The development of IOT devices, machine learning, and artificial intelligence ("AI") has given rise to the ability to collate and analyze larger amount of data, opening up possibilities to gain insights that can yield enormous societal benefits. Relying only on consent for the collection, use, and disclosure of personal data may have deleterious effects. India should instead adopt an approach that carefully calibrates the balance of responsibilities at issue in data collection and adopt preemptive measures that can meaningfully address concerns underlying the consent requirements.

The Draft Policy also claims that the "location of the computing facilities like data centers and server farms within country will not only give a fillip to computing in India but will also lead to local job creation." However, research shows that data localization policies are likely to hinder economic development,[6] restrict domestic economic activity,[7] and impede global competitiveness.[8] Rather than

[6] *See* Leviathan Security Group, *Quantifying the Costs of Forced Localization* (2015), http://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf (finding that "local companies would be required to pay 30-60% more for their computing needs than if they could go outside the country's borders"). Localization reduced GDP by 0.8% in Brazil, 1.1% in China, Korea, and the EU, 0.8% in India, 0.7% in Indonesia, and 1.7% in Vietnam. Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* at 6 (Sept. 2015), http://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20%20September%202015.pdf.

[7] Matthias Bauer et al., *The Costs of Data Localization: Friendly Fire on Economic Recovery*, ECIPE (2014), http://www.ecipe.org/media/publication_pdfs/OCC32014__1.pdf.

[8] Foreign investment will likely decline. Given the high cost of constructing data centers, many companies will simply opt out of serving markets with onerous data localization requirements, especially small and medium-sized businesses. In 2013, the average cost of data centers in Brazil and Chile were $60.3 million USD and $43 million USD, respectively. Loretta Chao & Paulo Trevisani, *Brazil Legislators Bear Down on Internet Bill Push for Data Localization*, WALL ST. J. (Nov. 13, 2013), http://online.wsj.com/articles/SB10001424052702304868404579194290325348688. *See also* U.N. Conference on Trade and Development, Data Protection Regulations and International Data Flows at 3, (2016), http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf ("[I]f data protection regulations go 'too far' they may have a negative impact on trade, innovation and competition."); Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION at 607 (May 2017), http://www2.itif.org/2017-cross-border-data-flows.pdf ("At the firm level, barriers to data flows make firms less competitive, as a company will be forced to spend more than necessary on IT services. Companies will likely have to pay more for data-storage services, especially those in smaller countries (which will not naturally be home to a data center). Such barriers also prevent companies from transferring data that's needed for day-to-day activities, such as for human resources, which means companies may have to pay for duplicative services.").

protectionist policies, India should pursue policies that allow local firms to access the global market.[9]

Trust in digital services plays a key role in furthering trade. However, provisions that promote cross-border data flows are not synonymous with lax privacy regimes, and the imposition of strict restrictions is not the best means by which to protect personal data of citizens. Further, firms are no less obligated to follow applicable laws regarding data protection just because a server is located outside a country.[10]

There are many examples of frameworks that allow for different approaches to privacy while still enabling data transfers necessary for essential business operations such as the APEC Cross-Border Privacy Rules and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. Similarly, all countries party to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP") recognize the importance of data flows to enabling trade and are committed to strong cross-border data transfer rules.

Localization can undermine the goals of privacy protection. Rather than ensuring user privacy or data security, forced localization creates a host of new targets of opportunity for hackers, criminals, and foreign intelligence agencies.[11] These requirements have the effect of decreasing data security. Restricting information technology services to a specific jurisdiction does not automatically increase data security, even if these policies give governments a false sense of control. Mandates to maintain local data centers frequently result in the establishment of minimally-resourced facilities that are more likely to permit network intrusions and data compromises. Instead, data security and adequate privacy protections are a result of investment and comprehensive operational strategies.

Compliance costs are ultimately passed on to consumers when prices for goods and services are increased in order to fund local outposts instead of having centralized service centers that maximize efficiency. Further, restrictions on data transfer often have a disproportionate effect on smaller businesses, in certain cases thwarting growth opportunities altogether and preventing today's startups from becoming tomorrow's multinationals. For many companies, the costs of compliance with localization mandates are prohibitive and deter market entry. This leads to fewer choices for individuals in India, with a pronounced impact on India startup companies that depend on access to low-cost cloud storage and computing services. In short, imposition of localization requirements as envisioned in the Draft Policy would be contrary to the goals of promoting a 'Digital India'.

---

[9] Access Partnership, *What UNCTAD Gets Wrong about the Digital Economy* (2018), *available at* https://www.accesspartnership.com/cms/access-content/uploads/2018/11/What-UNCTAD-Gets-Wrong.pdf?hsCtaTracking=dc307170-a4dd-4125-aac8-116ac37e3b09%7C48a6f8a2-53ac-4a54-9f3f-02c7a907c998.

[10] *Id*. at 6.

[11] Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 718-19 (2015), http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf; Silvia Baur-Yazbeck, *Three Myths About Data Localization*, CGAP (Aug. 21, 2018), https://www.cgap.org/blog/3-myths-about-data-localization ("Governments concerned about unauthorized access to sensitive data are better off requiring data security and encryption standards than mandating localization. For example, encryption can prevent any third party from accessing the data, including hackers, the cloud provider and the country where the data are located. Outsourcing data storage allows FSPs to make necessary investments in the operational security efforts that do protect against insider threats, such as access and user right controls, data encryption and awareness building").

B. The WTO Moratorium on Imposing Customs Duties for Electronic Transmissions

The Draft Policy also makes a number of comments on the WTO moratorium on customs duties for electronic transmissions and the ongoing WTO e-commerce negotiations. As a point of clarification, the Draft Policy states that the ongoing e-commerce negotiations intend to "create binding obligations on all the WTO member countries." CCIA supports this important work but notes that the current negotiations are plurilateral in nature and will only commit countries who have agreed to participate to the new rules.

The moratorium has been key to the development of global digital trade and reflects the international consensus with respect to the digital economy, reflected in the number of commitments made in free trade agreements among multiple leading digital economies. Permanent bans on the imposition of customs duties on electronic transmissions are also a frequent item in trade agreements around the world. This includes but is not limited to Article 14.3 of the CPTPP,[12] Article 19.3 of the U.S.-Mexico-Canada Agreement ("USMCA"),[13] and Article 8.72 of the EU-Japan Economic Partnership Agreement.[14] Further, as the moratorium has been renewed several times at the WTO, India cannot begin imposing customs duties on digital transmissions without violating its international commitments.

The Draft Policy's contemplation of ending the moratorium and extending customs duties for digitally-delivered services is in direct contravention to traditional customs norms and practices that treat only physical goods as subject to customs duties. Imported goods are subject to the levy of customs duties at the applicable levels under the Customs Act, 1962, and courts have confirmed that this is restricted to goods that physically cross jurisdictions. An expansion of the meaning of imported goods to include digital transmissions would require a change to both Indian law and changes to India's commitments under the WTO.

Imposing customs requirements on purely digital transactions will also impose significant and unnecessary compliance burdens on nearly every enterprise, including small and medium-sized enterprises ("SMEs"). The Draft Policy does not take into account the number of requirements that would accompany such an approach, many of which would be extremely difficult to comply with. For instance, data points required for compliance include the description of underlying electronic transfer, end-destination of the transmission, value of transmission, and the country of origin of the transmission — all of which do not exist for most electronic transmissions, especially in the cloud services market.

[12] Final Text of Comprehensive and Progressive Agreement for Trans-Pacific Partnership, signed Mar. 8, 2018, https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[13] Final Text of U.S.-Mexico-Canada Agreement, signed Nov. 30, 2018, https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf.

[14] Final Text of Agreement Between EU and Japan for Economic Partnership, http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf#page=185.

CCIA encourages the Government of India not to pursue national strategies that depart from the international consensus regarding the decisions not to impose customs duties on electronic transmissions.

III. Concerns with the Draft Policy's Approach to Data Governance

Policymaking should be conducted pursuant to rigorous analysis of economic evidence and models. In establishing the reasoning for its data strategies, the Draft Policy alternatively describes data in terms of "collective property," a "mine of natural resource," and "the new oil" and endorses property-style individual and collective ownership rules over information. However, these comparisons obscure and distort fundamental characteristics of both data and the digital economy. Reliance on these flawed analogies leads the Draft Policy to recommend market interventions that would limit consumers' control over their personal information and shrink market competition, innovation, and commerce. Rules for electronic commerce should be based on a clear understanding of personal information; how firms collect, process, and distribute data; and both the value and risks that digital practices pose to businesses and consumers.

A. The Draft Policy's Flawed Analogies on Data

Fundamentally, data is observable and measurable information that describes something about the world. In the e-commerce environment, businesses and consumers mutually benefit when firms leverage capabilities and tools to rapidly and efficiently collect and analyze consumer data. For example, data processing enables businesses to optimize prices, predict trends, reach new customers, and meet consumer needs more efficiently. It is important to recognize how the characteristics of data distinguish the digital economy from natural resource consumption and markets, and render regulatory frameworks based on property analogs ineffective and inefficient.

1. Data Is Not a Natural Resource

It is popular to mischaracterize data as a natural resource or commodity such as "the new oil."[15] At a high level, this framing may appropriately imply some of the innovation and economic benefits that have accompanied the emergence of the digital economy. However, on closer examination, the analogy breaks down for many aspects of data that are crucial for setting the standards for governing personal information.

First, unlike natural resources, data is infinite, reusable, and non-rivalrous. Natural resources like oil are expensive to collect and distribute, and are depleted through use. However, vast quantities of data can be collected, replicated, distributed, used, and reused with minimal additional marginal costs.

Second, data can be simultaneously used for multiple purposes throughout all levels of the economy and wider society. As stated, big data practices have brought about important innovations in e-

[15] *See, e.g.*, Antonio Garcia Martinez, *No, Data Is Not the New Oil*, WIRED (Feb. 26, 2019), https://www.wired.com/story/no-data-is-not-the-new-oil/; Jacob Kucharczyk, *Data is not the New Oil*, BLOGACTIV (July 19, 2017), https://blogactiv.eu/blog/2017/07/19/data-is-not-the-new-oil/.

commerce, but data can also be used for research, innovation, and insights in fields such as transportation, healthcare, and education. Big data collection and processing is also enabling innovative emerging technologies such as predictive analytics and artificial intelligence.

Third, data does not hold any intrinsic value. Commodity markets establish the price of a barrel of oil or an ounce of gold at any given time, but there is no "measurable value" that ties directly to any specific set of data points. Instead, the value of data is derived from the ability of a data controller to organize and process the information to discern meaning or solve a problem.

2. Ownership and Property Rights Are Inappropriate Frameworks for Protecting an Individual's Interest in Her Data

Building on mischaracterizations of data as a tangible and finite natural resource, the Draft Policy asserts that "[a]n Individual owns the right to his data." Consumers should hold rights with respect to personal data related to them, including the right to know how their personal information is collected, used, and shared and to exert certain controls over their personal information.[16] However, concepts of property and ownership are poorly suited to consumer information in digital commerce. Using these frameworks would create market inefficiencies and undermine efforts to empower and protect consumers.

First, the common law foundations for assigning property rights are not suitable for the digital space. E-commerce data relating to a consumer such as time spent on a website, items viewed, or purchase history is not generated solely through the effort of the consumer and any value in that data is produced through analysis conducted by the data controller. Therefore, even under a property rights framework, it is unclear how property ownership of different types of data should be assigned or distributed.[17] Furthermore, at its core, data is observed information, vesting the observer with free speech interests in their observations that are not compatible with the assignment of conflicting ownership rights.

Second, attempting to assign ownership rights over data would produce significant transaction costs resulting in serious market inefficiencies. Most consumers recognize that data collection and use is necessary to participate in e-commerce and are comfortable with most data processing pursuant to these purposes. However, assigning a property right to data and requiring that all data collection and use must be bargained-for would upend the digital economy, overwhelming consumers with cumbersome opt-in mechanisms, stifling the capacity for firms to use data in electronic commerce, and foreclosing innovation, competition, and investment.[18]

Finally, property harms such as trespass and damages do not have natural corollaries in a digital environment. A property rights-style data governance regime is therefore not well-suited to

[16] For example, the Personal Data Protection Bill, 2018 lays out important "data principle rights" such as confirmation and access, correction, and portability.

[17] *See* Bart Schermer, *Privacy and Property: Do You Really Own Your Personal Data*? (Sept. 8, 2015), https://leidenlawblog.nl/articles/privacy-and-property-do-you-really-own-your-personal-data.

[18] *See* Larry Downes, *A Rational Response to the Privacy 'Crisis'*, POLICY ANALYSIS (Jan. 7, 2013), https://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

effectively prevent or compensate for the actual risks of harm that can result from the misuse or improper disclosure of personal data.[19] Instead, e-commerce regulations should focus on maximizing data benefits and minimizing possible harms by promoting secure and appropriate data processing practices.

Given that analogies of individual data to a natural resource are inappropriate, it follows that regulating aggregate data as a collective resource or national asset would be similarly inefficient. While the Draft Policy is correct to recognize the importance of group level data and hints at the importance of open data, it advances an inappropriate framework for maximizing economic growth and socially beneficial data practices. Consumers should be empowered to exercise choice and assert their privacy preferences in the marketplace. A regulatory framework in which the government exercises a "sovereign right" to citizen data as a "trust" would limit consumer power and choice as well as market competition. Further, such a framework of government control would be in tension with the Supreme Court of India's recognition of personal privacy as an "intrinsic part of the right to life and personal liberty."[20] As explained in Section C below, the Draft Policy's approach to data ownership is also inconsistent with the Personal Data Protection Bill, 2018 and the conclusions reached by the Srikrishna Committee.[21]

B. Conflict with Global Consensus on the Role of Consent in Privacy Frameworks

Based on the Draft Policy's flawed conception of data as a natural resource meriting the assignment of ownership and property rights, the Draft Policy advances two concerning data governance strategies. First, that "if at all the data of an individual is used, it must be with his/her express consent."[22] Second, that sensitive data "stored abroad shall not be made available to other business entities outside India, for any purpose, even with the customer consent."[23] These contradictory proposals would, if enacted, substantially burden the digital marketplace and produce negligible, if any, benefits to Indian consumers and businesses.

1. Drawbacks to an Overreliance on Express Consent

Data subjects should be able to exercise reasonable control over data processing in the context of their relationship with digital commerce services. However, requiring express consent for every aspect of data processing is impractical and counter-productive. Such a mandate would overload consumers with opt-in requests, causing 'notice fatigue' and degrading the user experience. Consumers recognize that some level of data collection and use is necessary for the provision of

[19] *See* Testimony of Jane Bambauer, Hearing on GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation, U.S. Senate Judiciary Committee (Mar. 12, 2019), *available at* www.judiciary.senate.gov/imo/media/doc/Bambauer%20Testimony.pdf (explaining the problem associated with treating privacy as property).

[20] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C 1, *available at* https://www.sci.gov.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[21] Committee of Experts Report Under the Chairmanship of Justice B.N. Srikrishna, *available at* https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf, at 32-40.

[22] Draft National e-Commerce Policy, at 14.

[23] *Id.* at 16.

digital services. Therefore, if express consent is to be sought, it should be limited to situations involving the collection or use of sensitive personal information outside the context of a consumer's relationship with the digital service.

2. Restrictions on Third Party Data Processing

Draft Policy Strategy ¶ 1.2 would prevent businesses that collect or process sensitive data in India and store it abroad from making the data available to a third party, "for any purpose, even if the customer consents to it." By overriding consent, this proposed ban would constrict consumer's control over their personal information in opposition to the Draft Policy's goal of empowering consumers in digital commerce.

Furthermore, this strategy would be highly burdensome because many organizations, especially startups and small businesses, rely on data transfers to vendors and suppliers in order to provide services, authenticate user accounts, protect data security, and combat e-commerce fraud. Rather than adopting blanket bans on information practices, regulations should focus on promoting transparency and accountability. Through these principles, regulators can ensure that users understand the circumstances where their personal information may be transferred to a third party and that third parties comply with privacy and security obligations governing personal data. Adopting this approach would provide for synchronicity with global frameworks and provide for both user control and third party accountability while still enabling the data transfers necessary for business operations and a healthy competitive environment.

C. Inconsistency With Existing Regulatory Efforts in India

The Draft Policy sets out to fill regulatory gaps and ensure harmonious e-commerce policy across the Government. However, the Draft Policy's data strategies conflict with multiple provisions of India's Personal Data Protection Bill, 2018 ("the Bill"), which is intended to fulfill the Supreme Court's direction to enact a "robust regime for the protection of personal data."[24] This divergence threatens to create legal uncertainty for both businesses and consumers and undermine India's data protection regime. First, the Bill establishes a consent-based regime for personal data processing, without relying on a flawed property or ownership regime.[25] Second, the Bill requires in-country processing of only "critical" personal data, and the Ministry of Information and Technology has mentioned in public representations that this is intended to be a deliberative process and only limited categories of data will be notified in this manner. As the Draft Policy seeks to impose restrictions on various categories of data, the Draft Policy is not harmonious with the scheme of the Bill. Therefore, in order to promote a comprehensive and consistent data protection regime, the Draft Policy should be revised to align with these provisions of the Bill.

[24] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C 1, *available at* www.sci.gov.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[25] Draft Personal Data Protection Bill, Chapter VI, "Data Principle Rights."

IV. Concerns With the Regulatory Strategy on Data and Competition

Competition policy and antitrust enforcement play an important role in driving technological innovation. Crucial to an effective national competition strategy is a clear understanding of the underlying business models of complex digital services, and policy recommendations based on sound economic analysis. National policies that fail to account for market realities and that are based on flawed understandings of certain competition dynamics should be discouraged.[26]

A. Data as a Dimension of Competition

"Data" itself should not be viewed as a barrier to entry. Data does not automatically grant competitive advantage in the market. The value derived from data comes from the processing of data, not the mere accumulation.

The Draft Policy makes many incorrect assumptions regarding the role of data in the success of a firm. The key to gaining a competitive edge is not the accumulation of data but the capacity to analyze data. Research has shown that across technology companies, data did not grant incumbents power to strangle competition,[27] little user data is required as the starting point for most online services,[28] and that additional access to data provides diminishing returns to the accuracy.[29]

Mandated data sharing alone as if it were an essential facility (as envisioned in ¶ 1.4) will not enable startups. Mandatory data sharing involving data subjects also appears to conflict with the Draft Policy's notion that data subjects have ultimate control over their data. In order to build a vibrant startup economy, India should pursue a holistic strategy with measures that will incentivize innovation such as skill promotion and development, increased access to capital, and research and development incentives. Merely mandating data access from larger firms would not accomplish the stated long-term goals to develop the domestic digital economy. In fact, there is no legal foundation on which companies may be forced to part with such data. Rather India's intellectual property laws protect rights in datasets created by companies. Forced data sharing and other similar measures outlined in the Draft Policy would discourage investment in India and will force some firms to leave the market.

B. 'Network Effects' as They Relate to Competition in the Digital Economy

The Draft Policy refers to 'platforms' and 'network effects' throughout the document to discuss the perceived trend towards concentration in the digital economy. In lieu of these terms, the concept of

[26] The Draft Policy does not refer to ongoing committee review of India's Competition Act. This is concerning as many of the general conclusions made throughout the Draft Policy regarding competition are not accompanied by evidence-based analysis.

[27] David S. Evans & Richard Schmalensee, *Network Effects: March to the Evidence, Not to the Slogans*, Antitrust Chronicle (Aug. 2017) at 9, *available at* http://mitsloan.mit.edu/shared/ods/documents/?DocumentID=4243.

[28] D. Daniel Sokol & Jingyuan (Mary) Ma, *Understanding Online Markets and Antitrust Analysis*, 15 NW. J TECH. & INTELL. PROP. 43 (2017), *available at* https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1267&context=njtip.

[29] Stanford Dogs Dataset, *available at* http://vision.stanford.edu/aditya86/ImageNetDogs/.

'two-sided' or 'multi-sided' markets is better substituted for 'platforms' when considering competition issues involving 'platforms' that unite two or more separate groups of users in a marketplace.[30]

Multi-sided business models are enterprises based on a business model whereby the demands between different types of customers, connected by the platform, are interdependent. These business models, including certain online marketplaces, stock exchanges, dating websites, messaging platforms, and payment networks, enable two or more distinct sets of customers to interact with each other, realizing gains from such interactions. What characterizes these business models is that there is interdependency of demand between them. In other words, the demand for the platform's services by each set of customers depends on the demand for the platform's services by at least one other set of customers.

Network effects are present when the value of adopting a service to an incremental user is larger when more users have already adopted the service.[31] Network effects, or demand side economies of scale, are not unique to digital services.

The assumption that the existence of network effects precludes competition unilaterally is not accurate. The presence of network effects in competition analysis must account for whether 'single-homing' and 'multi-homing' aspects are also present.[32] 'Multi-homing' refers to instances where customers use more than one platform or services, and 'single-homing' refers to those instances where customers only use one platform or service in a given industry. Compared to legacy networks,[33] many of the current online platforms are more susceptible to disruption from new

[30] Daniel O'Connor & Matthew Schruers, *Against Platform Regulation*, Presentation Draft, Oxford Internet Institute Conference on Internet, Policy, and Politics (Oct. 2016) at 3-8, *available at* http://blogs.oii.ox.ac.uk/ipp-conference/sites/ipp/files/documents/OConnor-Schruers%2520-%2520Against%2520Platform%2520Regulation.pdf.

[31] *See, e.g.*, Hal R. Varian, *Use and Abuse of Network Effects* (Sept. 17, 2017), *available at* https://ssrn.com/abstract=3215488.

[32] *See* Justus Haucap & Ulrich Heimeshoff, *Google, Facebook, Amazon, eBay: Is The Internet Driving Competition Or Market Monopolization?*, Düsseldorf Institute for Competition Economics (Jan. 2013), *available at* http://www.dice.hhu.de/fileadmin/redaktion/Fakultaeten/Wirtschaftswissenschaftliche_Fakultaet/DICE/Discussion_Paper/083_Haucap_Heimeshoff.pdf.

[33] David Evans, *Why The Dynamics Of Competition For Online Platforms Leads To Sleepless Nights, But Not Sleepy Monopolies* (2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3009438 ("Online platforms are more susceptible to attack by entrants than network industries of a century ago. Network effects and sunk costs made the natural monopolies around the turn of 20th century difficult to challenge. Rivals had to sink massive amounts of capital into duplicating physical networks such as railroad tracks and telephone lines. Using multiple networks, or switching between them, was expensive for customers, even if a second network was available. However, online platforms can leverage the Internet to provide wired and wireless connections globally. People find it generally easy, and often costless, to use multiple online platforms, and many often do. The ease and prevalence of multihoming have enabled new firms, as well as cross-platform entrants, to attract significant numbers of users and secure critical mass necessary for growth. Incumbent platforms then face serious competitive pressure from new entrants—startups or other online platforms—because their network effects are reversible.").

entrants due to "lower barriers to entry, low switching costs, the prevalence of free-to-the-user business models, and multi-homing."[34]

C. Competition in the Online Advertising Market

The Draft Policy claims that "advertising charges in ecommerce must be regulated, especially for small enterprises and start-ups" based on "[t]he presence of network implies that a few social media platforms and search engines virtually control access to potential consumers" which "puts them in a position to charge monopoly prices also makes it very expensive for new firms, small enterprises and start-ups to reach consumers." This characterization does not accurately reflect the nature of competition in the online advertising market.

Over the past 20 years the Internet economy has disrupted traditional advertising models, bringing benefits to both advertisers and consumers. The Internet has lowered costs to advertise, offering many free services, and has enabled SMEs and small businesses to connect with audiences around the world at low to no cost. Search engines are a useful tool to return organic search results that allow users to connect with new and relevant services.[35]

Competition for consumer attention, and in turn, advertising revenue, remains fierce between mediums.[36] Even within the digital advertising market, platforms compete with a variety of services for user attention, all of which have the opportunity to display relevant advertising. This includes services such as messaging, gaming, streaming, various search engines, social media, and video, both on desktop and mobile, with new arrivals appearing regularly. Major media, telecommunications, and Internet competitors have expanded advertising revenue or are planning significant investments into the digital advertising market, while market leaders are expected to lose ground in the coming years.[37]

The Draft Policy contemplates regulating advertising charges by social media platforms and search engines due to 'high rates' charged. However ideas expressed in ¶¶ 4.6-4.7 suggest there is a lack of understanding on how digital ads operate on leading e-commerce services. For example, the costs of advertising in search results are often set by a bidding system, rather than a single firm setting

[34] *See* Haucap & Heimeshoff, *Google, Facebook, Amazon, eBay: Is The Internet Driving Competition Or Market Monopolization?*, *supra* note 32.

[35] Danny Goodwin, *Organic vs. Paid Search Results: Organic Wins 94% of Time*, Search Engine Watch (Aug. 23, 2012), https://searchenginewatch.com/sew/news/2200730/organic-vs-paid-search-results-organic-wins-94-of-time; Brightedge, *Organic Search Is Still the Largest Channel* (2017), https://www.brightedge.com/resources/research-reports/organic-search-still-largest-channel-2017.

[36] Matt Schruers, *Infographic: How Ad Dollars Are Spent*, DISRUPTIVE COMPETITION PROJECT (Jan. 16, 2018), *available at* http://www.project-disco.org/competition/011618-how-ad-dollars-are-spent/.

[37] Mark MacCarthy, *Competition in Digital Advertising is On the Rise*, CIO (Dec. 19, 2018), *available at* https://www.cio.com/article/3328650/amazon-com/competition-in-digital-advertising-is-on-the-rise.html; *see also* George P. Slefo, *IAB Says Digital Ad Revenue on Pace for $100B This Year, But Headwinds Loom*, AD AGE (Nov. 13, 2018), *available at* https://adage.com/article/digital/iab-digital-ad-revenue-catapults-49-billion/315598/.

"monopoly prices" (¶ 4.6). Further, in many cases digital advertising delivers a far higher return on investment than offline alternatives, which benefits SMEs.[38]

D. Disclosure of Source Code and Algorithms

The Draft Policy makes flawed assumptions about networks effects in the digital market, and uses these assumptions to justify a proposal to require access to source code and algorithms. However, source code and algorithms are often protected by trade secret frameworks and other intellectual property protections. Mandatory disclosure of these assets would raise significant intellectual property concerns. Disclosure of source code and algorithms is not necessary to promote the values of algorithmic and AI explainability. These mandates should be removed from the Draft Policy and India should not pursue similar measures as it seeks to develop a national strategy.

E. Preference for Domestic Cloud and Email Services

The Draft Policy proposes 'budgetary support' and other preferences for domestic alternatives to foreign-based cloud and email facilities (¶ 2.4). Instead, India should pursue alternative approaches to promoting India's digital economy. Strategies to spur innovation include collaborative R&D programs, public-private partnerships, the establishment of IP facilitation centers and incubators, training and recruitment assistance to MSMEs and grassroot innovators, and export promotion models that do not pose artificial barriers to foreign technology providers. Through these strategies, India can increase its competitiveness in global markets for cloud computing and email services. These strategies will also generate long-term benefits for India's economy, rather than short-term benefits that can arise through providing preference to local suppliers.

V. Concerns with Intermediary Obligations Regarding Third Party Content

Strategies with respect to intermediary obligations should be consistent with global norms and protections under current law. A key component of the Internet ecosystem is the understanding that intermediaries, including e-commerce platforms and websites, cannot police all content posted by third parties. A strong, innovative economy relies on certain protections that limit liability of intermediaries for the content posted by their users while enabling platforms to continue to deploy tools to enforce terms of service and remove unlawful content.

India has recognized this through the exemptions granted for intermediaries under Section 79 of the IT Act. The Supreme Court of India also provided welcome clarification regarding India's intermediary framework in *Shreya Singhal v. Union of India*, reducing regulatory uncertainty.[39] However, there are parts of the strategies outlined in the Draft Policy that could conflict with this

[38] *See Slefo*, *id.* ("Digital advertising is giving direct-to-consumer brands more agility to place effective and efficient ads at lower cost of consumer acquisition, the IAB says, adding that as long as consumer acquisition proves to deliver strong return on investment, marketers will continue increasing their spend for future growth.").

[39] Supreme Court (India), Shreya Singhal v. Union of India, (2015) S.C.C. 248, *available at* https://globalfreedomofexpression.columbia.edu/wpcontent/uploads/2015/06/Shreya_Singhal_vs_U.O.I_on_24_March_2015.pdf (reading Section 79(3) of the IT Act to require an intermediary to achieve actual knowledge and act only upon receipt of a court order to remove content).

understanding. Since current law states that an intermediary platform is not required to engage in proactive monitoring of content, or legally obligated to determine the legality of content hosted on its platform (or determine whether any third party content is infringing intellectual property), the approaches of the Draft Policy which advocate for proactive monitoring may be at odds with existing law.

The Department should clarify whether it is creating new obligations on a class of 'website[s] or e-commerce platform[s]', or whether this is restating current policy. This is relevant for the provisions outlined in the anti-counterfeiting obligations (¶¶ 3.9-3.17 and ¶¶ 3.18-3.20) regarding anti-piracy obligations. As the Ministry of Electronics and Information Technology is currently considering changes to the current Intermediary Framework, additional guidance is needed.[40]

The proposal under ¶ 3.20 regarding 'rogue websites' is also concerning. The identification and maintenance of the proposed 'Infringing Websites list' appears to take place outside judicial process, and it is not clear who the 'industry stakeholders' managing this process are. This could lead to blocking lawful content and restriction on free speech. Any framework should not allow for extrajudicial delisting or blocking of websites, and provide proper due process to any business accused of unlawful activity.

The Department should also clarify whether it intends to propose new obligations on 'online platforms' and 'social media' separate from existing law in Section IV of the Draft Policy. Intermediaries take seriously their roles under current obligations to remove unlawful content and have devoted significant resources on a voluntary basis to address rising concerns regarding misinformation and abuse online. However, is it not clear what responsibility to 'ensur[ing] genuineness' refers to in the Draft Policy, and an obligation to 'ensur[ing] genuineness' would likely be unfeasible to comply with.

VI. Concerns with Proposals Regarding Digital Taxation

If changes are warranted to global taxation, stakeholders should look to a global consensus model that does not ring-fence the digital economy. CCIA supports international, multilateral efforts to reach consensus on a lasting framework that accounts for the current state of global business.

India's desire to pursue the concept of 'significant economic presence' as the basis for determining 'permanent establishment' should be read in light of India's current obligations under its Double Tax Avoidance Agreements which define 'permanent establishment' differently.

The discussion regarding international taxation reform should be separate from the discussion regarding the WTO moratorium on imposing customs duties on electronic transmission (discussed on page 6), not as a way to recoup perceived lost revenue.[41]

[40] CCIA's comments regarding the proposed amendments to the Intermediary Guidelines are available at http://www.ccianet.org/wp-content/uploads/2019/02/Comments-of-CCIA-to-MeitY-on-Draft-Intermediary-Guidelines-2018-1.pdf.

[41] The notion that the existing moratorium on customs duties on electronic transmission is causing a revenue loss does not account for the fact that under existing Goods and Services Tax laws in India, the exchange of electronic

VII. Conclusion

While it is encouraging that the future of the digital economy is a priority of the Government of India, CCIA is concerned that a number of proposals envisioned in the Draft Policy will have severe consequences for India's domestic economy and pose significant market access barriers. CCIA encourages the Department to provide further clarification and guidance on how these strategies will interact with existing legislation and regulatory frameworks.

transmission of data for consideration is covered. As such, electronic transmissions that are made to a taxable online recipient for consideration would attract a goods and services tax. Calls for the elimination of this moratorium in order to increase revenue are then misplaced.