BSA Submission
on
Draft National E-Commerce Policy

Shri Goonjan Kumar,
Assistant Director,
Department for Promotion of Industry and Internal Trade,
Ministry of Commerce and Industry,
Udyog Bhavan, New Delhi – 110011

March 29, 2019

Dear Sir,

Subject: BSA Submission on Draft National E-Commerce Policy

BSA | The Software Alliance (**BSA**)[1] appreciates this opportunity to comment on the Draft National E-Commerce Policy (**Policy**) prepared by the Department for Promotion of Industry and Internal Trade (**DPIIT**).

BSA is the leading advocate for the global software industry and actively follows trade-related developments around the world. Our member companies are at the forefront of data-driven innovation, and they have a deep and longstanding commitment to protecting the privacy and security of personal information. BSA has been active in India for over a decade, working closely with Central and State Governments on issues important to the software industry. Our member companies invest substantially and have extensive operations in India, developing cutting-edge technology solutions, products, and services in India, as well as establishing world-class R&D centers and generating jobs in India.

[1] BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Le-Meridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

At the outset, we would like to thank the DPIIT for issuing a call for public consultation on the important issue of e-commerce policy in India. BSA agrees that unlocking India's innovative potential requires an effective e-commerce policy framework that promotes trust in the digital economy. To that end, we welcome the efforts by DPIIT to acknowledge the role of data protection, infrastructure development and a wider legal framework in the formulation of a meaningful E-Commerce Policy. BSA and its members have been closely following and contributing to the Government of India's efforts to develop a comprehensive policy for the data economy including the development of a robust data protection regime in India to promote the use of artificial intelligence and to enhance the use of cloud computing across sectors.

Although many aspects of the Policy would lay a strong foundation for a robust regulatory framework in India, several of the proposals would pose substantial challenges that would restrict the ability to provide customers in India with the most seamless and secure digital services. Thus, while the issues discussed below do not account for all of BSA's concerns about the Policy, they highlight the provisions that, in BSA's view, would create the greatest difficulties for businesses that offer services to India as part of a dynamic, innovative, and global digital economy. Most importantly, these proposals are inconsistent with the Policy's underlying goal of accelerating the pace of innovation of within India's digital economy.

1. Cross-Border Data Flows

The seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. Global data flows enable multinational companies to scale global operations, start-ups to use cloud services to obtain digital infrastructure at lower costs, and small- and medium-sized enterprises to use digital platforms to find customers and suppliers abroad. Cross-border data flows are particularly important in the area of cybersecurity, enabling distributed and compartmentalized data storage, as well as allowing correlation of threat data for more effective cybersecurity defense.

Cross-border data flows are essential to fuel data analytics, which can deliver socially and economically beneficial results in situations ranging from digital commerce to responses to natural disasters. For example, in 2015, researchers around the world conducted a real-time analysis of mobile phone patterns to assist in disaster relief efforts in the wake of the devastating earthquake in Nepal.

Therefore, the proposed restrictions on cross-border transfers involving data collected by IoT devices or otherwise generated by users in India (Paragraph 1.1) as well as the stringent conditions on uses of data stored abroad (Paragraph 1.2) are extremely problematic and should not be included in the Policy. Paragraph 1.3 exempts certain classes of data from the cross-border transfer restrictions (e.g., data not collected in India, B2B data sent to India as

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

part of a commercial contract, software and cloud computing services which have no personal or community implications, and internal MNC data shared across borders when it does not contain data generated from Indian users). However, because it is impossible to predict how technologies will evolve, such a "whitelist" approach that permits cross-border transfers of only specific categories of data will inevitably become quickly outdated, creating a risk that Indian users will be denied access to technological solutions that are driving the digital economy in other markets. Indeed, applying the restrictions of Paragraph 1.1 and 1.2 to anonymized data and data needed for enhancing cybersecurity threat detection and response, to name two categories of data not explicitly mentioned in Paragraph 1.3, would harm business and consumer security interests today.

Notably, the scope of localisation measures – in terms of the kind of data that is sought to be localized, overlap with sectoral regulations and the Draft Personal Data Protection Bill 2018 (**PDP 2018**) - envisaged in the Policy remains unclear. Restrictions on data flow sought to be imposed by the Policy not only reduce the scope of data transfer under the present law, but also do not align with the PDP 2018. This risks the creation of parallel frameworks for the transfer of similar varieties of data, and conflicting legal regimes which may lead to low enforcement and a potentially unstable business environment.

PDP 2018 enumerates specific principles concerning the use, processing, storage and transfer of personal data. We recommend DPIIT to evaluate these principles specifically in the context of this Policy.

Restrictions on the cross-border transfer of data and data localisation requirements do not advance the goals stated in the Policy. Instead, they disrupt companies' operations and make it costlier to provide services in India.

According to Gartner, the revenue from public cloud services in India was projected to grow at 37.5% to total USD $ 2.5 billion in 2018.[2] The proposed restrictions on cross-border transfers would threaten this national economic growth, as these types of restrictions often impose significant costs on the countries that adopt them. For instance, data localisation measures have a negative economic impact on GDP,[3] with one study estimating that data localisation measures could have an -0.8% impact on GDP in India. The study also concludes that data

[2] India's Public Cloud Revenue to touch $2.5 billion this year: Gartner by The Economic Times, available at: https://economictimes.indiatimes.com/tech/internet/indias-public-cloud-revenue-to-touch-2-5-billion-this-year-gartner/articleshow/64093963.cms

[3] *See* White Paper of the Committee of Experts on a Data Protection Framework for India, at 70,

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

localisation measures negatively affect exports for several countries, resulting in a -1.7% export loss in both Indonesia and China.[4]

Data localisation requirements also raise the cost of providing services in the country to which the requirements apply, potentially increasing costs for end consumers. Data localisation requirements may also put a dent on the ambitious 'Start Up India' campaign of the Government of India, as such burdensome regulatory requirements disproportionately impact small and medium-sized enterprises (SMEs) that may not have the necessary resources to ensure compliance when they leverage global services. Further, data localisation may prevent local start-ups from choosing and using services at affordable rates, leaving them with fewer and more expensive choices resulting from a lack of effective competition. Studies also indicate that local companies would be required to pay 30-60% more for their computing needs in such cases.

As referenced above, data localisation requirements would also inhibit competition and the choice of technology available to end-users and procuring entities, including start-ups and government agencies. Any legal mandate that requires data to be hosted within India would eliminate many data storage options from those available in the global market. It is simply not practical for providers to have all of their services and functionality available in every country, since part of the cost savings and efficiencies that cloud service providers are able to offer result from economies of scale, which often require data be stored in multiple locations. Even where a particular provider has hosting facilities in India, because of how such platforms are configured, it is likely that some features or functionality will require certain data to be stored outside of India. In many cases, it is not possible to process all data locally with the same quality of service as could otherwise be achieved – for example, with respect to certain fraud detection services. Therefore, it becomes important that DPITT undertakes a detailed study on cost-benefit analysis of adopting a conservative approach for cross-border data flows.

Additionally, the restrictions on data flow have been enacted with regard to "sensitive" data – without defining what kind of data qualifies as sensitive in the context of the Policy. Notably, the Policy does not refer to the SPDI Rules under the Information Technology Act, 2000 and the definition of "sensitive personal data and information" contained therein. Thus, the scope of data sought to be protected by the Policy is unclear.

Keeping in mind the need for a vibrant and competitive digital ecosystem in India, it is important to formulate policies that promote access to digital products and services at competitive prices. This would enable Indian businesses and start-ups to participate in global supply chains and directly access customers in foreign markets.

---

[4] European Centre for International Political Economy, *The Costs of Data Localisation: Friendly Fire on Economic Recovery*, at 6 (2014), available at http://ecipe.org/publications/dataloc/

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

2. Anonymised Data

The Policy states – "*Even after data is anonymized, the interests of the individual cannot be completely separated from it*."

BSA recommends excluding anonymized data from coverage of the Policy. The PDP 2018 defined anonymised data as "data that is not reasonably linkable to a specific individual." By definition, such data is not personal and therefore does not implicate individual privacy interests. The freedom to use adequately anonymised data would benefit all players in the eco-system, including individuals and the overall economy. The provision of an exclusion to such data would give businesses the incentive to develop and use anonymisation techniques, thereby reducing privacy and security risks. At the same time, the ability to use anonymised data outside the Policy will encourage wide-ranging innovative uses of data beneficial to all forms of Indian firms and users.

3. Consent Framework

BSA is concerned that the Policy recommends the adoption of an "explicit consent" requirement for all forms of processing involving the "data of an individual." Those concerns are compounded by the Policy's additional suggestion that certain forms of processing should be prohibited even when a user has provided adequate consent.

Consent is a crucial basis for handling user data. The standard for obtaining consent should be contextual to determine the level of consent that is appropriate. In circumstances that do not implicate heightened sensitivity, implied consent may also be appropriate.

In today's world, a large amount of data is created through individuals' interactions with Internet-connected devices, and express consent is not suitable or practical in all instances. For example, the future of public transportation services may be affected if an individual must provide express consent to allow an electronic gate to generate data every time he or she swipes a public transportation card. In other circumstances, such as the handling of sensitive health or financial data, affirmative express consent may be appropriate. The Policy, thus, should consider this context and allow sufficient flexibility for determining the timing, standard, and mechanism for obtaining consent. Such flexibility may be significantly hindered due to the Policy's stance regarding the treatment of data even after the obtaining of explicit consent.

As reflected in various legal frameworks across the world, including the EU General Data Protection Regulation (**EU GDPR**) and the PDP 2018, the processing of data for legitimate or reasonable purposes without explicit consent has been acknowledged and is in conformity with global regulatory standards. The approach outlined in the Policy is unlikely to achieve the

Policy's stated objectives. Instead, this approach will result in unintended consequences that are likely to disrupt the Indian economy.

In addition to our concerns with the "express consent" requirement, we are concerned by the Policy's proposed prohibition on certain forms of data processing. For instance, the Policy suggests that the sharing of "sensitive data" with third party entities should be prohibited "even with customer consent." Respecting individual autonomy means that individuals should be able to control and share their personal information as they wish. By prohibiting an individual from consenting to specific uses of his or her data, the Policy would be inconsistent with the underlying purpose of a data protection regime. As the Supreme Court in ***K.S. Puttaswamy*** vs. ***Union of India***[5] explained:

"*177..Apart from safeguarding privacy,* ***data protection regimes seek to protect*** *the* ***autonomy of the individual****. This is evident from the emphasis in the European data protection regime on the* ***centrality of consent****. Related to the issue of consent is the* ***requirement of transparency which requires a disclosure by the data recipient of information pertaining to data transfer and use****.*"

4. Collective Ownership and Compulsory Access to Data

In an effort to promote data innovation in India, the Policy suggests that data generated by Indian users should be regarded as "collective property" and treated as a "national resource that should be equitably accessed by all Indians."

Although we agree that data will be key to growth in all sectors of the economy, these proposals will drive up the costs of the value-added services that help transform data into a valuable resource. The reality is that individual pieces of data have very little inherent value in isolation. It is only when such data is used as an input to other value-added services, such as Artificial Intelligence (AI), that it contributes to the projected $15 trillion addition to global GDP by 2030.[6] Policies that artificially increase the costs for acquiring the data used to train AI systems will ultimately increase the costs of these technologies for customers and decrease the incentive to develop and use new technology — potentially reducing overall consumer welfare.

The Government of India should therefore pursue policies that facilitate the business-to-business exchange of data and boost the development of AI services, including by:

- Ensuring companies are free to enter enforceable contracts that create data sharing arrangements on mutually agreed terms;

[5] (2017) 10 SCC 1.

[6] BSA, What's the Deal with Big Data, available at http://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf.

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

- Avoiding the creation of new rights in business data that could add unnecessary transaction costs; and
- Allowing companies to freely perform data analytics, including text and data mining, on any content to which they have lawful access.

The Government of India should likewise avoid creating compulsory access policies. Creating and structuring data sets is resource intensive. A regulatory prohibition on maintaining the exclusive benefits of that investment will deter the investment and impede the development of AI in India.

The Policy's suggestion that there should be a "sovereign right" over data would create similar problems. As a practical matter, it is unclear how ownership of an item over which there is a "sovereign right" would be ascertained. The Policy suggests that data ownership should be treated similarly to a natural resource, such as a "coal mine," because "data about an Indian is his/her own" and therefore should not be "extended to non-Indians." The Policy thus seems to suggest that ownership of data would vest simultaneously with the state (like a coal mine) and with individual end-users. Such a layering of rights would introduce tremendous uncertainty and undermine fundamental principles about the nature of data protection.

5. Compelled Disclosure of Source Code and Algorithms

Paragraph 4.10 urges the Government to establish a policy for compelling disclosure of source code and algorithms from companies operating and developing AI systems. We agree that ensuring the accountability of AI systems is an important issue. BSA supports this objective. However, compelling the disclosure of source code or algorithms is an ineffective method for ensuring accountability of AI systems. Research has shown that requiring disclosure of algorithms, or associated data sets is ineffective in helping to provide explanations of an system, in part because they cannot be meaningfully understood in isolation.[7] We therefore encourage the Government of India to focus on promoting accountability of AI systems through approaches that would provide a broader understanding of how AI systems operate, but which do not otherwise require the disclosure of confidential business or other proprietary information. The Government of India should support such efforts, which are far more likely to address relevant concerns than broad, one-size-fits-all disclosure mandates that may pose privacy and other concerns, while not addressing the primary question of increasing public understanding of these systems. Such measures could give customers sufficient confidence in the unbiased nature of the AI-driven software, while ensuring that proprietary interests in the software are not compromised.

[7] *See* Kartik Hosanagar & Vivian Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire,* Harvard. Bus. Review, July 23, 2018, *available at* https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire.

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

6. Customs Requirements on Electronic Transmissions

BSA recommends that India proceed with due care in relation to any suggestion to impose customs duties on electronic transmissions. India benefits from a significant comparative advantage in software development and IT services relative to most other countries around the world, and therefore stands to lose significantly if other countries begin imposing additional restrictions in the form of customs requirements on software-enabled electronic transmissions.

BSA also submits that it may be misplaced to claim that, "the GATT schedule of countries will erode and will vanish ultimately," and that "[Indian] nascent industries in the digital arena will disappear at once." The rapid growth of India's software and IT services sectors has occurred almost entirely in a marketplace in which customs requirements were not imposed on these sectors. India could face significant loss of export markets and negative job impacts, as well as the loss of future export growth opportunities, if its numerous export markets increase restrictions on Indian product or services imports, including through the imposition of customs requirements.

7. Incorporation Requirements

The Policy proposes to mandate that all e-commerce platform and service providers to incorporate in India as a precondition to providing services in India. A local incorporation requirement is not only trade restrictive, it would also deprive consumers of the flexibility that has been offered to them through the development of various innovative e-commerce platforms that provide technology services on a cross border basis while connecting consumers and goods/service providers locally.

8. Anti-Piracy Measures

The Policy proposes a number of requirements that are intended to limit the distribution of infringing content. BSA members are highly innovative companies which rely on intellectual property protections as the basis of their business models. Like other desirable content, software is subject to high volumes of online infringement. Accordingly, BSA members appreciate the importance of workable legal frameworks that afford rights holders with meaningful tools to prevent the distribution of infringing content. At the same time, BSA members also operate cutting-edge cloud services, and in that capacity operate as online intermediaries. BSA members therefore understand the importance of ensuring that the legal framework includes limitations on liability to ensure intermediaries are not required to implement intrusive measures to monitor their users of filter their networks – obligations that would undermine users' privacy rights, weaken incentives for innovation, and threaten the dynamism that have made the internet so valuable.

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

The anti-piracy measures proposed by the Policy would undermine the balance that has enabled the growth of India's digital sector. The proposed requirement to "prevent online dissemination of pirated content" would apply to all "intermediaries." To the extent this proposal is intended as a requirement to proactively monitor and/or removal of content, it would conflict with established law. For instance, in ***Shreya Singhal*** vs. ***Union of India,***[8] the Supreme Court concluded that an intermediary cannot be required to proactively monitor its platform for unlawful content, and its responsibility is limited to actioning content when notified by court orders or authorized government agencies. The Delhi High Court likewise concluded in ***Kent RO Systems Ltd. & Anr.*** vs. ***Amit Kotak & Ors***[9] that intermediaries cannot not be required to proactively remove content pursuant to the IT Act because they are ill equipped to make legal determinations about whether content is infringing.

9. Competition

The growth of the digital economy has transformed business operations in virtually every industry sector. To ensure that the existing competition policies remain fit for purpose in the digital era, the Government of India recently established a Competition Law Review Committee to perform a comprehensive study of the evolving business environment.[10] Such a study will enable the Committee to make evidence-based recommendations to ensure that India's competition framework is serving the public interest. This study remains ongoing and DPIIT should refrain at this time from including recommendations related to competition in the Policy.

* * * *

Thank you for providing BSA the opportunity to participate in this meaningful consultation process. We hereby also share the following documents for your reference

1. *What's the Big Deal with Data* – a report by BSA | The Software Alliance[11]
2. *Comments of BSA | The Software Alliance on "The Personal Data Protection Bill, 2018"* on September 2018[12]

---

[8] (2013) 12 SCC 73.

[9] CS (COMM) 1655/2016.

[10] *See* Government constitutes Competition Law Review Committee to review the Competition Act *available at*: http://pib.nic.in/newsite/PrintRelease.aspx?relid=183835

[11] *See* What's the Big Deal with Data *available at***:** https://data.bsa.org/wp-content/uploads/2015/12/bsadatastudy_en.pdf

[12] *See* Comments of BSA | The Software Alliance on "The Personal Data Protection Bill, 2018" *available at***:** https://www.bsa.org/~/media/Files/Policy/Data/09282018BSACommentsonIndiaDataProtectionBill.pdf

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org

We thank you for providing us with the opportunity to participate in this meaningful consultation process. We hope our submissions are useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion and stand ready to answer any questions you may have.

Yours sincerely

Venkatesh Krishnamoorthy
Country Manager- India
BSA | The Software Alliance

Le-Méridien
15th Floor, Room 1529
Windsor Place, Janpath
New Delhi 110001
India

P (91 11) 4978 9066
W bsa.org