29 March 2019

New Delhi

To,

1. Mr. Ramesh Abhishek,
   Secretary
2. Mr. Goonjan Kumar
   Assistant Director

Department for Promotion of Industry and Internal Trade (DPIIT)
New Delhi - 110022

Subject: Response to Request for Comments on Draft National E-Commerce Policy dated February 23, 2019

Dear Sir,

Koan Advisory Group ("Koan") is a New Delhi-based policy advisory firm. Our team combines thorough domain knowledge across multiple sectors with continuous engagement of decision makers across industry and government. We specialise in policy and regulatory analysis in both traditional and emergent sectors and markets, with the aim of identifying optimal frameworks that maximise societal welfare.

We are delighted to be afforded the opportunity to respond to the Department for Promotion of Internal Trade and Industry's (DPIIT) Draft National E-Commerce Policy (Draft Policy). Our response keeps in mind the overarching policy targets of a USD one trillion digital economy, which can sustain 60 to 65 million jobs by 2025 as articulated by the Ministry of Electronics and Information Technology (MeitY)[1]. Specifically, MeitY underlines that the "*potential benefits of digitisation are contingent on India's ability to generate efficiencies in production and distribution on a mass scale, which will require regulatory and policy changes coupled with a* ***significant increase in digital investment by government, private enterprise, and individual stakeholders***".

In addition, we are cognisant of the fact that through the National E-Commerce Policy, India also aims to delineate its stance on e-commerce related discussions at the multilateral level (World Trade Organisation), and at bilateral and plurilateral (Regional Comprehensive Economic Partnership Agreement) trade discussions. In this context, the following sections respond to some of the proposals in the Draft, keeping in mind India's existing obligations under international instruments, and the domestic legal framework.

DATA: With respect to treatment of data, and related questions of ownership of data and cross-border transfers, the Draft will need to be harmonised with established Constitutional jurisprudence, and forthcoming frameworks and policies including the Draft Personal Data Protection Bill, 2019 (PDP Bill) and the proposed amendments to the Intermediary Guidelines under Section 79 of the Information Technology Act 2000. Presently, the Draft takes an inconsistent position on the ownership of data. On the one hand, it emphasises the autonomy and ownership of individuals over their data while recommending that corporations processing such data without explicit consent

[1] Ministry of Electronics and Information Technology, India's Trillion-Dollar Digital Opportunity, February, 2019; available at https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

must be dealt with sternly. At the same time, it proposes provision of access to datasets containing data of Indian users to MSMEs and start-ups without addressing how consent will be obtained for this.

Further, it disregards explicit consent of the data subject while restricting transfer of sensitive data stored abroad to any third parties. In so doing, it likens data to a societal commons, where national data is "*a national resource to be accessed equitably by all Indians".*

Evaluating the Draft's Rationale for Societal Commons and Public Trust Doctrine: First, it is important to unpack the categorisation of data as a societal commons akin to a natural resource. Here, let us consider notions of "res communis" or common heritage of mankind. Typically, items which fall under such categories tend to be resources which cannot be directly linked to a particular individual, community, or sometimes even the country. In public international law common examples of the same include outer space, international waters, etc. Some other examples of such societal commons can include the environment, spectrum or rare earth minerals. Evidently, it is difficult to ascribe private ownership to such resources given certain innate characteristics—which make ownership untenable for a functioning society. On the other hand, ownership of a particular data set can be ascertained either to an entity which has created that data set, or to the various individuals who have granted access to their personal data through a specific consent mechanism for a specific purpose. Therefore, such a characterisation of Indian data being a national asset/resource akin to a societal commons, does not appreciate the individual centricity of data (even when it has been anonymised), and in the case of aggregated data sets, the specific proprietary rights of the entities that develop such data sets.

Moreover, the draft's contention that the government should hold Indian data in trust and direct its allocation based on principles articulated under the public trust doctrine is flawed. Since we are discussing the applicability of the doctrine to data and future technological conversations— it is appropriate to understand this doctrine as applied to spectrum, which is integral to the domain of the telecommunications sector—an allied domain to the sector the draft seeks to govern. Supreme Court judgements like the *Airwaves case*[2] and the *2G Spectrum*[3] *case* clearly discuss that the public trust doctrine is invoked in domains such as spectrum due to notions of resource scarcity. It is due to this resource scarcity that government assumes control over the resource, and then determines its allocation in a manner which optimises public/societal good.

This is even evinced under India's Telegraph Act, 1885. Under Section 4 of the Act, the only entity which is allowed to operate a telegraph unimpeded is the Government of India. Moreover, due to such spectrum scarcity, government tightly controls access to players to operate telegraphs in India.[4] However, as economies and telecommunications continue to enter future technological paradigms—current views on spectrum scarcity and licensed access to spectrum are undergoing review. Illustratively, both the Indian Department of Telecommunications (DoT) and telecom authorities abroad are examining strategies to improve spectrum utilisation, spectrum management and create increased avenues to utilise spectrum through unlicensed means.

Here, it is important for policymakers to acknowledge that challenges of scarcity are not applicable to data as data is inherently infinite and replenishable in nature. Thus, without such scarcities, the justification of invoking the public trust doctrine to data originating from Indian users is conceptually misplaced.

---

[2] *Ministry of Information and Broadcasting v. Cricket Association of Bengal* 1995 2 SCC 161.
[3] *Centre for Public Interest Litigation v. Union of India* 2012 (3) SCC 1.
[4] Section 4, Indian Telegraph Act 1885.

Contradictions with Established Human Rights Jurisprudence: The extant approach further contradicts the emphasis on individual control and consent and foundational aspects of data privacy as laid out in the *Puttaswamy* judgement which recognised privacy as a fundamental right. The *Puttaswamy* judgement conceptualises privacy as a fundamental right which is intrinsically related to an individual's practice of their rights under Article 14 (Equality), Article 19 (Freedom of Speech and Expression) and Article 21 (Right to Life and Liberty). These fundamental rights accrue to their holders in an individual capacity, and seek to empower individuals as well as protect them from excesses of the State. As the majority opinion in *Puttaswamy* states, *"Privacy is a concomitant of the right of the individual to exercise control over his or her personality. It finds an origin in the notion that there are certain rights which are natural to or inherent in a human being. Natural rights are inalienable because they are inseparable from the human personality. The human element in life is impossible to conceive without the existence of natural rights…"*[5]This comes from a long line of rights jurisprudence based in natural law, which recognises that rights inhere in individuals by virtue of them being human, and are not bestowed by a State or authority. Recognising the natural origin of human rights, the Supreme Court in the milestone case of *Maneka Gandhi v Union of India*[6] noted that even in an era where rights were thought of as products of socio-political processes, they could not be morally divorced from the notion of certain inherent rights: "*...the idea that man, as man, morally has certain inherent natural primordial inalienable human rights goes back to the very origins of human jurisprudence.*"[7] Further, any restrictions on such rights could only be allowed when there is a statutory law to this effect and the restriction is valid both in its reasoning and procedure - '*If either the reason sanctioned by the law is absent, or the procedure followed in arriving at the conclusion that such a reason exists is unreasonable, the order having the effect of deprivation or restriction must be quashed.*'[8] Therefore, the conceptualisation of privacy as a community-oriented right is blind to the wealth of rights jurisprudence laid down and followed by courts in the country.[9]

This aspect of privacy has been denoted in the Srikrishna Committee Report as well, which recognises ***that all information about a person is fundamentally owned by that person***. Further, while noting that there might be particular cases where there is a countervailing interest in fostering a free and fair digital economy, it states that a judicial determination by a Court is required to arrive at the correct position. Therefore, since this involves a fundamental rights analysis, application of a judicial mind is imperative, and cannot be theorized by an executive body such as the DPIIT.

Community Data:

---

[5] *Ibid.* para 118

[6] 1978 AIR 597

[7] *Ibid.*para 19

[8] *Ibid*. para 28

[9] In *Tamil Sakthi vs The State Of Tamil Nadu*, [W.P(MD)No.5145 of 2005] , the Madras HC described human rights as - "*Human rights are derived from dignity and are inherent in human beings. Human rights are natural rights which come by birth as human beings which are basic, indivisible, inalienable and inherent with which a person is born. Broadly speaking, human rights may be regarded as those fundamental rights which are possessed by every human being. Such rights by their free nature constitute the minimum that is necessary for an individual to live in civil and political society as a free person with dignity and respect."*; In *R.Karuppaiah vs The Superintendent Of Police* [HABEAS CORPUS PETITION (MD) No.291 of 2007], the Court observed that - "*Human rights are derived from dignity and are inherent in human beings. Human rights by their very nature, constitute the minimum that is necessary for the individual to live in a civilized society as a free person with dignity and respect in that society. These rights are positive in nature and as they make it the duty of the State to ensure for realisation of these rights.*"

The Draft, using the example of traffic data collected at intersections, asserts that such collections of data are collective property. It goes on to say that 'the data of a country' is a national asset that the government holds in trust. It cites APIs for Aadhaar, BHIM, eKYC and the Goods and Services Tax (GST) Network as sources of such data, while underlining in the same breath the need to give citizens control over their own data. It recommends the development of a suitable framework for sharing of community data (subject to privacy-related issues) with start-ups and firms, with implementation up to a 'data authority' (presumably the Data Protection Authority mentioned in the PDP Bill). This reveals a misunderstanding of the concept of community data introduced in the Srikrishna Committee Report.

Revisiting the concept of Privacy as a Public Good: The Srikrishna Report relies on a 2015 paper[10] to *recommend a suitable law to include a principled basis for protection to identifiable communities, including class action remedies, and tools like group communication and sanction.* This paper itself considers approaches to privacy protection *that empower groups and protect privacy* ***without direct government intervention*** *through institutionalising tools for communication and private sanction*[11] (which have been picked up by the Report). The Paper refers to schemes wherein identifiable groups, for instance a particular indigenous community in an area, can evolve their own mechanisms for data governance, such as a data governance council. This will help create institutions which serve as conduits for groups managing their own data instead of it being held and managed by government. Thus, the academic concept has been misapplied in the Draft to recommend government control over such data. Additionally, the examples provided in the Draft, such as the Maori Data Sovereignty Network, cannot be applied to India. This is a specialised policy for an indigenous group and subject to specific rights articulated in the Treaty of Waitangi between the British colonisers and the indigenous people of New Zealand. **As such, it is part of the right to self-determination exercised by indigenous groups, with a distinct and autonomous legal tradition, and thus offers them sovereignty over their data.** Nation states bound by their domestic legal frameworks and international conventions cannot adopt a similar approach.

Re-emphasising consent: If the objective of the Draft is to create an ecosystem where data can be shared between processing entities, it must do so keeping consent and autonomy at the core of any such system.

The *Puttaswamy* judgement emphasised: "*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.*"[12]

The Judgment also relies on the Canadian Supreme Court case of *R. v Dyment*[13], where it was held that seizure by police of a blood sample taken for medical purposes and subsequent use of the same as evidence in a drunk driving case was violative of privacy. Therefore, use of personal data of individuals without their consent as envisaged in Strategy 1.1 (of the Draft Policy) as well as restrictions on consent-based transfer in 1.2 are likely to be violations of the right to privacy under *Puttaswamy* and therefore unconstitutional.

---

[10] Joshua Fairfield and Christoph Engel, Privacy as a Public Good, 65(3) Duke Law Journal (2015)

[11] *Ibid.* p. 396

[12] Para 171, *supra* note 2.

[13] 1988 2 SCR 417.

The centrality of consent and autonomy is emphasised in the Srikrishna Committee Report. Here, even as it creates exceptions for government use of personal data without obtaining consent, it stresses the importance of tailoring this exception narrowly. It states that only two kinds of functions may be allowed to fit under this exception - i) for the provision of services and subsidies in the nature of welfare benefits and ii) to the extent necessary for performance of regulatory functions. It goes on to say, "*A large part of the functioning of various departments of Government may be indirectly or remotely connected to the promotion of public welfare or regulatory functions. The ground cannot be used to justify the processing of personal data for all such functions. For functions not covered under this ground, the State, like other private actors, must rely on consent as the ground for processing personal data.*"[14] Further, it is made clear that even such collection must follow the principles of collection limitation and purpose limitation, i.e. collecting only as much data as necessary for fulfilling a certain purpose and using it only for that purpose.[15]

Drawing from existing domestic models: In India, an example of such a consent-based data sharing system can be found in the RBI's recognition of certain Non-Banking Financial Companies as Account Aggregators.[16] These allow users to digitally share their financial data with service providers for easier access to financial products, or just to keep track of their investments. NBFC-AAs, as they are called, act as a consent dashboard -- using user consent to access their financial data and sharing the same with any service providers when users consent to such sharing. They are not allowed to use or access any customer information other than for the business of an account aggregator explicitly requested by the customer.

International Best Practices: Models for data sharing in other jurisdictions, too, enshrine consent as a central feature.

The **UK**'s Open Banking Directive, which came into force in January 2018, requires nine banks – HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds and Nationwide – to release their data in a secure, standardised form, so that it can be shared more easily between authorised organisations online. The system is set up by a non-profit called Open Banking Limited, and the Competition & Markets Authority handles enforcement. Banks are responsible for consumer protection when it comes to payments related concerns, and the Information Commissioner's Office, analogous to the Data Protection Authority (DPA) envisioned in the PDP Bill, handles data-related concerns. It aims to empower users with regard to their financial data and promote competition and innovation in the banking sector. Regulated apps and websites can offer open banking services -- acting as a consent dashboard where users can view all their financial data, as well as authorise sharing of such data with particular financial institutions they want to transact with. This has served the purpose of innovation within the market, with new services such as simplified rental agreements through expedited credit checks being offered. At the same time, it respects user autonomy and makes data sharing easier while incorporating a consent framework.

France, too, has sought to obtain greater strategic access to datasets in order to consolidate its data sovereignty and capitalise on the rise of AI. Its National AI Strategy[17] focuses on the importance of data for machine learning and the development of AI capabilities, and the need to unlock the data potential of France. However, it does not do this through coercive means such as compelling companies to part with data, rather recommends incentivizing open data and data pooling. Here, the

[14] Report of Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, p. 111

[15] Section 5, Draft of Personal Data Protection Bill, 2018.

[16] Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016

[17] https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

government plays a facilitative role by organising 'Data Forums' where private entities can come together to discuss the mutual and reciprocal benefits that can be accrued from a robust open data ecosystem. It also talks about leveraging the Right to Data Portability under the EU General Data Protection Regulation (GDPR) in order to develop a citizen-based rationale for greater data sharing between private entities for the benefit of the entire economy.

The **European Union** is also looking at the Directive on Open Data and Public Sector Information to increase the availability and re-use of public sector data across the EU. The underlying principle of open data is that government held information (such as census, survey, applications, tax documents etc) is collected from the public, and such collection is also paid for by the public. Thus, there must be greater public ownership of such data. Therefore, the public, under the Open Government License (OGL) may copy, modify, publish, translate, adapt, distribute or otherwise use the information in any medium, mode or format for any lawful purpose. Licensees are required to identify the source of data on their derived products. This is expected to increase the potential for AI and machine learning products and represents the respect that the EU has for citizens' privacy.

Competition Concerns: The Impact Assessment accompanying the proposal for the EU Directive points out that sharing of publicly held data with select entities (through exclusive arrangements etc.) leads to distortion of competition in the market by providing certain companies with a competitive advantage. Therefore, it has recommended against selective sharing of publicly held data, and instead allowing wider access to such data. Such concerns would also apply in the Indian context, where the disincentives for foreign players in the form of the competitive advantage held by Indian firms would make them less likely to invest resources towards innovative uses of the data which are beneficial to the public. It is worth noting that the biggest share of FDI in India, at 17.5% is in the services sector[18] (including financial and banking services, insurance etc.), which relies on processing the data of Indian consumers. This would also be negatively impacted by such a move.

- *Restrictions on Cross Border Flows:*

The Draft proposes '*the creation of a legal-technological framework for imposing restrictions on cross border flow of data collected by IoT devices in public spaces and data generated by Indians on e-commerce platforms, social media sites and search engines'*. It also proposes that sharing of sensitive data of Indians stored abroad with business entities located abroad, foreign governments or other third parties be prohibited, even in cases where the customer consents to the same.

The Report, which examined the issues at play in the creation of a data protection framework recognises that the individual has the right to protect one's identity and further that an individual is free to communicate or retain it per their choice. *"This core of informational privacy, thus, is a right to autonomy and self-determination in respect of one's personal data. Undoubtedly, this must be the primary value that any data protection framework serves."* The Report further specifically upholds the principle of transfer of data on the basis of consent, while underlining that explicit consent will be needed for sensitive personal data. These recommendations are also reflected in the **Personal Data Protection Bill, *which allows for cross-border transfers of personal data with consent (including sensitive personal data with explicit consent) in Section 41*** in the following cases:

(a) subject to standard contractual clauses or intra-group schemes that have been approved by the Data Protection Authority.
(b) The Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible

[18] https://dipp.gov.in/sites/default/files/FDI_Factsheet_12March2019.pdf

(c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity.

All such conditions are disregarded in the Draft's treatment of personal data stored abroad, severely restricting the rights of individuals over their own data.

A total restriction on cross-border transfers of data designated as sensitive personal data, as envisaged by the Draft, would limit the ability of Indians to participate in the larger global digital economy, which relies on these flows to offer, optimise and deliver goods and services. For instance, it can inhibit a firm's ability to create data redundancies. This increases single point of failure risks and threatens network availability. Further, restrictions on cross-border data flows threaten the security of domestic and international financial networks, as most global service providers leverage big data analytics and artificial intelligence techniques to monitor global transaction flows in real-time to detect network anomalies at a global scale.

In addition, restrictions in cross-border data flows diminish the development of network security research across the global community which lends a clear advantage for malicious actors to exploit. Illustratively, a proposed 2013 amendment to the Wassenaar Arrangement (an international export control regime) specifically sought to restrict the cross-border flows of "intrusion software". However, such an approach brought to light certain challenges toward network and information security. Specifically, international security experts were adamant that such measures impede cross border knowledge sharing and technology transfers which are the corner stone of cyber security research and development. Further, such governance approaches do not keep in mind how cybersecurity companies develop their products using methods such as cross-border penetrative testing and that such provisions would increase the vulnerabilities across critical information infrastructure.[19]

It will also restrict the access of Indians to goods and services from around the world as they will not have the option to enter into contracts of their own free will, vitiating their freedom to contract and autonomy.

Intellectual Property Concerns:

Mandating private data processors and collectors to part with the data they've collected from consenting consumers is violative of their intellectual property rights (IPRs). When raw-data is compiled, arranged, processed and analysed, such databases acquire a proprietary nature due to the effort and innovation put in by the processor. The copyrightability of databases has been settled by the Supreme Court in *Eastern Book Company v. DB Modak*[20]. Here, the question was whether the petitioner, a company which created databases of Supreme Court cases (which are in the public domain) could claim copyright protection for their databases. It was held by the Court that the petitioner's input of independent skill, labour and capital, in editing and arranging the information as well as adding inferences from it in the form of headnotes, resulted in the database being a copyrightable work. This rationale would also apply to databases created and used by data processors as these involve skill, labour and capital investment in arrangement of the data, as well as drawing inferences from the data through processing. In view of this, compelling private entities to

19

https://poseidon01.ssrn.com/delivery.php?ID=520006116096074013079098106068122005120037062046029025071064112071068123074070094005018107016026040058048091066085102102098115040072009047028108106124093125000101086089069047098112116122002093121085109101020096029112005017094094113120120097031074065121&EXT=pdf

20 2008 1 SCC 1

share their datasets would completely disregard their copyright and be contrary to the law as settled by the Supreme Court. While the raw-data about individuals is owned by the individuals as noted above, the datasets consisting of such raw-data having been arranged and organised through input of labour and capital by private entities becomes proprietary to them.

The Draft summarily dismisses the use of Fair, Reasonable and Non Discriminatory (FRAND) terms and a compulsory licensing scheme as possible frameworks on the incorrect assumption that there is no element of ownership of private entities in these datasets. However, as demonstrated above, these datasets are proprietary in nature, and sharing these requires the development of new frameworks to enable a data rich economy.

To understand why FRAND is a model worth considering for such transfers, one may consider how it functions in the domain of Standard Essential Patents (SEPs). SEPs are patents in technologies that are prescribed by Standard Setting Organisations (SSOs) to be used across all products of a certain specification for compatibility and interoperability. In order to balance between access to these essential technologies and the rights of those who have developed them, the FRAND system of licensing is used. This prevents patent holders from discriminating between entities desirous of using these SEPs and at the same time ensures that they receive royalties for their investment in the development of the patent. Transplanted to proprietary data sets, this system could be enable greater access to data while remaining cognizant of the intellectual property rights of entities holding such data.

Similarly, compulsory licensing, which has been given statutory recognition in the Indian Copyright Act 1956 under Section 31, allows licensees to communicate to public copyrighted works even in the absence of consent of the rights-holder, provided they pay the statutory royalty. The rationale behind compulsory licensing typically is to promote the related industry and prevent monopolies, and in effect balance copyright holders' interests with the objective of fair access to protected works. Considering that *Eastern Book Co.* has already established the copyrightability of such datasets, compulsory licensing could also be explored as a means of sharing data. Such frameworks will need to be accompanied by the development of standards prescribing specifics such as data quality standards, formats and machine readability to ensure interoperability and ease in transfer of data sets. Further, privacy protecting provisions such as obligations upon transferee entities and privacy by design in the architecture of such a framework.

The Draft further buttresses this argument by asking whether individuals would be expected to pay entities for access to their own data. This is a fallacious and misleading characterisation. Individuals already own their own raw data and have access to it at all times - sharing the same with private entities does not preclude or diminish their access or prevent them from sharing the same data with another entity if they so wish. A good analogy can be found in medical testing - individuals may submit a medical sample to a diagnostics lab for testing. The individual then pays the entity not for the sample itself, but for the results of processing done on the same by the lab using technicians and equipment. Similarly, individuals will not be coerced into paying for their own data in a scenario where these and other means to balance access and intellectual property rights are considered.

- *IoT: Need for Standards*

The Draft's recognition of the growing relevance of IoT devices and the need to develop standards for consumer protection, interoperability and transaction security is timely and welcome. With more IoT devices being deployed in both private and public spaces, it is imperative to address related privacy and security considerations. In developing such standards for India, government may rely on emergent processes in other jurisdictions. The National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce has examined this issue in some depth, noting how

privacy must be approached from a different perspective for IoT than it is for traditional IT. This is due to the differences in technology, with IoT devices interacting with the physical world and collecting and transmitting large quantities of data, as well as the lack of user interfaces as elaborate and granular as in traditional IT. In a document called Considerations for Managing Internet of Things Cybersecurity and Privacy Risks[21], the NIST has stressed the importance of protecting individual privacy through the development of standards. This, according to the report, can be achieved through cybersecurity standards which prevent unauthorised access to personally identifiable information. In this regard, privacy has been found to be linked inextricably with cybersecurity. It has pointed out that while manufacturers focus on functionality, compatibility and time-to-market, a focus on security within consumer IoT software, firmware and data is missing. In addition to standards for interoperability, data security must be emphasised to ensure that IoT devices can be used without attracting the severe privacy risks associated - for instance unauthorised access to an IoT device collecting personal data in a home or public place.

The UK's Department for Digital, Culture, Media and Sport has also acknowledged the centrality of privacy in developing standards for IoT devices and software. In its Code of Practice for Consumer IoT Security[22], it includes ***ensuring that personal data is protected*** as one of 13 guidelines. This requires any devices/services processing personal data to do so in accordance with applicable data protection law, such as the GDPR and the UK's Data Protection Act 2018. The guideline specifically instructs service providers to provide consumers with clear and transparent information about the use of their data, including by any third parties (such as advertisers). It also holds that when processing on the basis of consent, such consent should be validly and lawfully obtained, and the consumer should have the option of withdrawing it at any point. It further includes a guideline to ***make it easy for customers to delete personal data*** from devices and services, including providing clear instructions to consumers on how to delete personal data.

The International Telecommunications Union (ITU), a UN agency which assists in the development and coordination of worldwide technical standards, has also underlined the protection of individual privacy as amongst the high level requirements for the development of IoT.[23] In the same recommendation, the ITU notes how data sensed by IoT devices may contain private information of owners or users, and there is a need to support privacy protection during data transmission, aggregation, storage, mining and processing.

It is clear that nations at the forefront of IoT technology as well as international organisations involved in the evolution of standards have stressed on the importance of respecting and protecting individual privacy while developing and deploying IoT technology. This recognition is missing in the Draft, which sees IoT technology simply as a means to collect and utilise more data. This narrow perspective must be reoriented to include the protection of privacy, and standards developed domestically as well as internationally must incorporate privacy friendly functions and mechanisms, some of which have been described above. India must engage with standard setting processes on the international stage too, in order to learn from best practices as well as to represent its own interests and needs in the creation of international standards.

---

[21] https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

[23] Recommendation Y. 4000, International Telecommunications Union (available at: https://www.itu.int/rec/T-REC-Y.2060-201206-I)

FOREIGN DIRECT INVESTMENT (FDI): At the outset it must be noted that a relatively open foreign investment (in India) policy has thus far played a vital role in the development of internet businesses in general, and the start-up ecosystem in particular. Moreover, given the lack of credit access, high cost of capital, and conservative approach adopted by financial institutions towards riskier investment, several Indian e-commerce entities presently rely on foreign private equity/venture capital for funding to scale up their businesses. For instance, in 2016 the Securities and Exchange Board of India's Alternative Investment Advisory Committee Report stated that (in India) a mere 10-15 per cent of equity capital required by start-ups, medium enterprises and large companies is funded from domestic sources. The remaining 85 per cent – 90 per cent is sourced from overseas. This is in contrast to the U.S. and China where domestic sources fund 90 per cent and 50 per cent respectively.[24] Therefore, it is important that India continue to actively encourage foreign investment.

Towards foreign investment, the Draft Policy states that under the existing foreign investment norms, FDI is permissible (upto 100 per cent under automatic route) only under 'marketplace' model, subject to stringent conditions. These include – marketplace should not exercise ownership over the inventory; barring entity having equity participation by marketplace or its group companies; and prohibition from influencing prices.[25]

In this context, it is important that the Policy clarifies the a*pplicability of FDI Policy on digital services:*

Similar to the WTO's Work Programme on Electronic Commerce, the Draft defines *e-commerce to include buying, selling, marketing, or distribution of goods, including digital products and services through electronic network***.** In contrast, the extant FDI Policy on e-commerce restricts the definition of e-commerce to 'buying and selling' of goods and services, consequently; leaving out services which are provided free of cost; or entities distributing digital product or services such as online audio-visual content providers.

In addition, it is important to note that the extant FDI Policy for e-commerce, subject to certain conditions, allows 100 per cent foreign investment through the automatic route in the market-place model of e-commerce (Para 5.2.15.2 of the E-commerce linked FDI Policy as amended by Press Note. 2 of 2018). ***Pertinently, with respect to digital services in general* (other than those services explicitly specified Consolidated FDI Policy), *investment is permitted up to 100 per cent under the automatic route, without being subject to any condition (Para 5.2 (a) of the Consolidated FDI Policy – the umbrella framework for FDI in the country)***.[26]

Therefore, we submit that DPIIT should refrain from expanding the existing definition of e-commerce under the FDI Policy, without revising extant FDI policies substantively. This would entail a thorough assessment of on-ground FDI that has already been permitted under automatic route by virtue of not being in the "prohibited list" of FDI services (as per para 5.2(a) of the Consolidated FDI Policy). In this context, government would be well advised to take a liberal and practical approach by recognising the continuing legitimacy of such investments and the need for a stable operational environment.

Furthermore, it must be highlighted that change in foreign investment conditions in the country should be in consonance with India's obligation under international investment agreements. This

---

[24] Securities and Exchange Board of India, Alternative Investment Advisory Committee Report, 2016; available at https://www.sebi.gov.in/web/?file=https://www.sebi.gov.in/sebi_data/attachdocs/1453278327759.pdf#page=1&zoom=auto,-16,792

[25] Press Note. 2 of 2018; available at https://dipp.gov.in/sites/default/files/pn2_2018.pdf

[26] Clause 5.2 (a) of the FDI Policy states that for sectors/activities which are not listed, 100 per cent FDI under automatic route is allowed, given that the sector/activities do not fall under the prohibited list; available at https://dipp.gov.in/sites/default/files/CFPC_2017_FINAL_RELEASED_28.8.17_1.pdf

legal position was recently endorsed by the Delhi High Court in ***Union of India v. Vodafone Plc*** wherein it held that India should not invoke its internal or domestic law as a justification for its failure to perform its international obligations.[27] Pertinently, most of the Bilateral Investment Treaties (BITs) of which India is a part contain 'national treatment' and 'fair and equitable treatment' clauses, which while prohibiting the country to discriminate between domestic and foreign investment, obligate it to maintain a predictable and stable legal environment.

Additionally, while interpreting fair and equitable treatment clause under BITs, the International Centre for Settlement of Investment Disputes in ***Tecmed v. Mexico[28],*** held that the such an obligation requires Contracting Parties to provide treatment that does not affect the basic expectations that were taken into account by the foreign investor to make the investment. The tribunal specifically held that *foreign investor expects the host State to act consistently, i.e. without arbitrarily revoking any pre-existing decisions or permits issued by the State that were relied upon by the investor to assume its commitments as well as to plan and launch its commercial and business activities.*

Notably, Indian BITs follow the post-establishment or post-entry model, consequently providing no general rights of admission and establishment. To put it differently, India's obligation to provide national treatment, and fair and equitable treatment does not extend to the admission and establishment stage of foreign investment.[29] However, these obligations do come into effect when foreign investment has already been admitted in India and is in play.

Even-though, in 2017 India terminated 58 BITs including the ones with countries such as Germany, France, and the United Kingdom[30]; ***investments made before the termination of the 58 treaties are nevertheless protected for 10/15/20 years under the 'sunset' clauses in those BITs.*** 'Sunset' clauses essentially stipulate that a treaty will continue to be effective for a further period from the date of the termination in respect of investments made before that date. For instance, the India–Netherlands BIT[31] provides that the substantive protections will continue to apply for fifteen years after termination for investments made prior to termination. Many of India's other treaties, such as those with the UK, Germany and Mauritius, contain similar 'sunset' clauses.

Apart from BITs, India's obligation under bilateral trade agreements also prohibits it from adopting a discriminatory regulatory requirement for entities of other parties.

For example, the India-Korea FTA, containing an exhaustive provision on 'national treatment', states that *"[e]ach Party shall accord to investors of the other Party treatment no less favourable than that it accords, in like circumstances, to its own investors with respect to the establishment ... of investments in its territory."* Similar provisions can be found in the investment chapters of the India-Singapore Comprehensive Economic Cooperation Agreement (CECA)[32] and the India-Malaysia CECA[33].

---

[27] Union of India v Vodafone Plc and Ors, CS (OS) 383/2017, available at http://lobis.nic.in/ddir/dhc/MMH/judgement/07-05-2018/MMH07052018S3832017.pdf

[28] Teccnicas Medioambientales Tacmed S.A. v. The United Mexican States, Case No. ARB (AF)/00/2; available at https://www.italaw.com/sites/default/files/case-documents/ita0854.pdf

[29] Press Information Bureau, Communication from Ministry of Commerce and Industry, available at http://pib.nic.in/newsite/mbErel.aspx?relid=87836

[30] http://164.100.47.190/loksabhaquestions/annex/12/AU169.pdf

[31] India – Netherland Bilateral Investment Treaty; full text available at http://investmentpolicyhub.unctad.org/Download/TreatyFile/1584

[32] Chapter 6, India – Singapore Comprehensive Economic Cooperation Agreement; available at http://commerce.gov.in/writereaddata/trade/ceca/ch6.pdf

[33] Chapter 10, India – Malaysia Comprehensive Economic Cooperation Agreement; available at https://fta.miti.gov.my/miti-fta/resources/Malaysia-India/MICECA.pdf

Presence of the term 'establishment' in trade agreements indicates its application as a pre-entry model. In other words, as per these provisions, India has agreed to national treatment obligations to foreign investment even before investment has entered the country, while in-general adhering to parity in post-establishment obligations across the board.

Therefore, alterations in the regulatory framework which adversely impact existing businesses might bring legal claims against the country under BITs. We recommend that the scope of existing FDI framework for digital services (other than those services explicitly specified Consolidated FDI Policy) should not be amended in any manner that inequitably impacts businesses operating in the country.

DIGITAL PRODUCTS: While the e-commerce definition under the Draft Policy mentions 'Digital Product', it fails to clarify which goods or services which fall under this category. Notably, even the existing legal frameworks in the country like the FDI Policy, and the Information Technology Act, 2000, does not contain a specific definition with respect to Digital Products. This has resulted in confusion regarding the ambit of the Draft Policy itself. Therefore, it is imperative that the future e-commerce policy contains a cogent definition of 'digital products.'

In this regard, definition of digital products in various trade agreements can provide essential guidance. For instance, the India-Singapore CECA provides that digital products include computer programs, text, video, images, sound recordings and other products that are digitally encoded, regardless of whether they are fixed on a carrier medium or transmitted electronically.[34] Furthermore, the agreement contains a footnote clarifying that the term does not include a digitised representation of a financial instrument. Similar definitions of digital product can also be found in other trade agreements like the Comprehensive and Progressive Agreement for Trans Pacific Partnership (CPTPP)[35], Korea-US FTA[36], and Singapore- Australia FTA[37].

While adopting/clarifying the scope of digital products under the Policy, DPIIT must be mindful that concomitant clarifications/amendments should also be effectuated towards applicability of provisions such as those related to consumer protection (as discussed below), and FDI Policy (as discussed above).

In light of the above, we submit adopting following definition for digital products:

Digital Products means goods or services which can be consumed only in electronic or digital format – which includes text, video, computer programmes, images, and sound recording.

- *Custom Duty on electronic transmission:*

With regard to custom duty on electronic transmission, the Draft Policy calls for reviewing the existing practice of not imposing tariffs.

The existing practice of moratorium on custom duty flows from decision taken by WTO's Member Countries under the forum's 1998 Work Programme on E-Commerce.[38] Importantly, the moratorium has been renewed in every Ministerial Conference, including in the last Ministerial Conference -

[34] Chapter 10, India – Singapore Comprehensive Economic Cooperation Agreement; available at http://commerce.gov.in/writereaddata/trade/ceca/ch10.pdf
[35] Article 14.1 of the Comprehensive and Progressive Agreement for Trans Pacific Partnership; available at https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf
[36] Article 15.9 of the Korea – US FTA; available at https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file816_12714.pdf
[37] Chapter 14, Article 1 of Singapore – Australia FTA; available at https://dfat.gov.au/trade/agreements/in-force/safta/official-documents/Documents/safta-chapter-14-171201.pdf
[38] World Trade Organisation's Work Programme on E-Commerce, 1998; available at https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

MC11, held in December 2017 in Buenos Aires, Argentina.[39] Furthermore, this moratorium on customs duty has become one of the foundational pillars of e-commerce chapters in various bilateral and plurilateral trade agreements including India-Singapore CECA.

It is pertinent to note that India currently does not levy customs duty on electronic transmissions, partly due to the existing moratorium agreed by it at the WTO, and partly due to its obligation under the India-Singapore CECA.[40] This moratorium applies only to digitised delivery of services or digital products like e-books and music, and not to goods which are traded over the internet and delivered in physical form.

However, as noted above, the Draft Policy calls for revisiting the existing practice of moratorium on custom duty. The Draft Policy's intention to revisit the moratorium appears to be on the basis of loss of revenue to the exchequer, and the impact on domestic manufacturing due to development of new technology such as additive manufacturing (commonly referred to as 3D printing).[41] Indeed, these concerns of unintentional extension of moratorium on custom duty to physical goods, are legitimate. For instance, technological advancements in 3D printing could potentially create an unlevel playing field or disparity while importing a product in physical form, and electronic (digital) format.

Nonetheless, it must be highlighted that imposing custom duties on electronic transmission might be undesirable for primarily two reasons: (a) it can undermine the free nature of the World Wide Web. For instance, a consumer might have to pay additional charge in the form of custom duty if he/she subscribes to foreign newspapers or journals; (b) even if custom duty on electronic transmission is levied, the enforceability of the same remains unclear. It is possible that cost of implementation of the duty will be more than the revenue gained from its imposition. Additionally, government must be mindful that India's IT/ITES industry has been able to flourish partly due to non-imposition of custom duty on electronic transmission, therefore, any decision to revise the status quo should be undertaken only after a detailed consideration of its impact on the IT/ITES industry, and on e-commerce entities as a whole, if other jurisdictions follow suit.

We would also like to highlight that method of imposing custom tariffs on electronic transmission under the existing multilateral framework – WTO's General Agreement on Tariffs and Trade (GATT), and WTO's General Agreement on Trade in Services (GATS) – remains unclear. Notably, WTO member countries are yet to agree on the legal treatment/classification of digital products under GATT or GATS.

Such classification is important due to the nature of these Agreements – for instance, the GATT framework is applicable to international trade in goods, while the GATS is applicable to international trade in services. Furthermore, while both Agreements largely provide for similar types of protection there are certain crucial distinctions. Firstly, GATT protections apply equally to all international trade in goods (market access and national treatment obligations are not dependent on specific commitments), GATS framework, per contra applies only to services for which Members States have made a specific commitment to be bound by the agreement (market access and national treatment obligations are based on specific commitments). Secondly, protections under GATT are generally in the form of custom tariffs, while that under GATS are in the nature of regulatory restrictions, such as those provided under India's FDI Policy.

---

[39] Ministerial Decisions, 11th Ministerial Conference; available at https://www.wto.org/english/thewto_e/minist_e/mc11_e/mc11_e.htm

[40] Article 10.4 of India – Singapore CECA; available at http://commerce.gov.in/writereaddata/trade/ceca/ch10.pdf

[41] South Centre, The WTO's Discussion on Electronic Commerce, SC/AN/TDP/2017/2; available at https://www.southcentre.int/wp-content/uploads/2017/01/AN_TDP_2017_2_The-WTO%E2%80%99s-Discussions-on-Electronic-Commerce_EN-1.pdf

To illustrate the dichotomy of classification of digital products – the European Commission states[42] that 'electronic deliveries consist of supplies of services which fall within the scope of the GATS'; while the United States has argued[43] that *'there may be an advantage to a GATT versus GATS approach to [digital] products which could provide for a more trade-liberalizing outcome for electronic commerce'*. Thus, any decision to impose tariffs might not be in consonance with India's commitments at the WTO, due to uncertainty regarding applicability of existing GATT/GATS norms.

Therefore, we recommend that India should continue to refrain from imposing custom duties on electronic transmissions of intangible goods or services i.e. goods that cannot be converted into physical form (Digital Products). Furthermore, to address concerns related to additive manufacturing, we recommend that government consider formulating a negative list (which can be amended when required), identifying the products which do not fall within the ambit of digital products. This will provide India the requisite flexibility to incorporate 'products' which were not envisaged to be governed such as delivery of digitised product for additive manufacturing.

- <u>*Non-discriminatory treatment of digital products*</u>:

We note that the Draft Policy provides for promoting domestic alternatives to foreign-based cloud and e-mail facilities. While we welcome the Department's intent to facilitate domestic industry, it must be careful to ensure that such measures do not result in unfair discrimination against foreign players. As India prepares itself to discuss trade rules on e-commerce at the WTO, and other bilateral and plurilateral for a, such as Regional Comprehensive Economic Partnership; it is important to note that one of the most common provisions found in trade agreements, which contain a stand-alone e-commerce chapter is to ensure that parties do not discriminate between digital products based on origin.

Pertinently, even the India-Singapore CECA also contains a similar provision which states that:

> "*Party(ies) shall accord to the digital products of the other Party treatment no less favourable than it accords to its own like digital products in respect of all measures affecting the contracting for, commissioning, creation, publication, production, storage, distribution, marketing, sale, purchase, delivery or use of such digital products".*

Similar wordings are also found in trade agreements like the TPP, Australia-Singapore FTA, Korea-US FTA and Japan-Mongolia FTA.

Apart from India's existing obligations under the India-Singapore CECA, it must be recognised that adopting discriminatory treatment against foreign players will impact the Indian digital economy in two ways: (a) it will restrict consumers' ability to access services of better quality/technology; and (b) it will adversely impact the local start-up ecosystem if other countries follow suit and start discriminating against digital products originating from India. This can potentially undo several years of innovation and fragment technology markets irreversibly. Recognising this, India presently does not discriminate between 'digital products' on the basis of product origin.

The Draft Policy, however, envisages preferential treatment to Indian origin digital products. While such preferential treatment for specific activities like government procurement is advisable, India should resist adopting measures which discriminate between foreign origin, and Indian origin digital products. Furthermore, as noted above, under the India-Singapore CECA, India is under obligation to adopt non-discriminatory measures; the provisions suggested in the Draft Policy could end up

[42] Council for Trade in Services, Communication from the European Communities and their Member States: Electronic Commerce Work Programme, S/C/W/183 (Nov. 30, 2000).
[43] Work Programme on Electronic Commerce: Submission by the United States, WT/COMTD/17

encouraging jurisdiction-shopping – wherein foreign players will rout the transmission of digital products via Singapore.

DISCLOSURE OF SOURCE CODE: Source code refers to the computer language which forms the backbone of software applications. The Draft Policy in this regard states that Government should reserve its right to seek disclosure of source code.

This approach appears to be driven primarily by concerns regarding inclusion of source code related obligations in some of the new-age trade agreements. For instance, the Comprehensive and Progressive Agreement for Trans Pacific Partnership has included an obligation on governments not to mandate access/disclosure to source code as a condition on allowing the import, distribution, sale or use of such software, or of products containing such software, in its territory.[44] However, it is important to note that the TPP provision is not applicable to government procurement, and to the software used in critical infrastructure.[45] In addition, the Agreement provides that a Party can require modification of source code of a software necessary for that software to comply with laws or regulations.

Inclusion of a blanket provision regarding government's right to seek source code disclosure, without any procedural safeguards or guidance behind the need for such disclosure, can adversely impact innovation, besides creating a barrier for market access. Notably, source code and algorithms are the intellectual property of the owner or the developer and hence inherent to the owner's right to do business and pursue his/her profession. In India, source code is protected under the extant Copyright Act, 1957.[46] Furthermore, the Supreme Court of India in the case of *Tarun Tyagi v. CBI (2017)*[47], has reiterated the position that the source code of a programme is the property of the person developing it and it cannot be surrendered in ordinary circumstances.

It is important to note that the focus of commercial software providers is on the functionality, features and innovativeness of their technology to meet the customer's needs, as their revenue model is based on the customer licensing their software. Customers purchase new versions of software when it provides new functionality, features and value. This incentive drives a tremendous flow of research and development spending into new software, the results of which include higher productivity, lower costs of business, and new tools for learning.

With respect to disclosure of source code for transfer of technology (ToT), the DPIIT should instead adopt measures to facilitate development/adoption of open source software (OSS) - software program that permit parties other than the original programmer to freely access the underlying source code of the programme.[48] Arguably, one of the popular examples of such an agreement is GNU's General Public License[49] (GNU-GPL). GNU-GPL is an agreement entered into between the creator of a software and its user which allows the user to do more than just consume software. The user is permitted to run, study, change, modify and distribute the modified the programme but he/she is prohibited from closing or restricting a software that was co-operatively developed.[50]

---

[44] See Article 14.17 of the CPTPP; available at https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf .
[45] *Ibid.*
[46] Section 14 (b) (ii) of the Copyright Act, 1957.
[47] Tarun Tyagi v. Central Bureau of Investigation, AIR 2017 SC 1136
[48] Neeraj R.S., Trade Rules on Source Code- Deepening the Digital Inequities by Locking up the Software Fortress, Centre for WTO Studies Working Paper; available at http://wtocentre.iift.ac.in/workingpaper/Working%20Paper%2037.pdf
[49] GNU Operating System, Licenses; available at https://www.gnu.org/licenses/
[50] *Id. 99*

Pertinently, government has adopted range of policies exist to push forward open source adoption and technologies in India, including:

- *The National Policy on Information Technology, 2012*: Among other things the policy aims to promote the 'adoption of open standards and promotion of open source and open technologies';[51]
- *Policy on Adoption of Open Source Software for Government of India*: the erstwhile Department of Electronics and Information Technology formulated this Policy to encourage the formal adoption and use of open source software in government organisations.[52]

Against this backdrop, we recommend that the Indian Government should refrain from adopting blanket provisions regarding mandatory source code disclosure of commercial software, which is devoid of necessary procedural safeguards. Alternatively, government should continue to facilitate adoption of OSS.

CONSUMER PROTECTION:

Presently, the Consumer Protection Act 1986 (CPA) governs the relationship between consumers and service/goods providers. There are no separate consumer protection rules or regulations that specifically regulate e-commerce. Pertinently, given that the CPA was enacted in 1986, it was not envisaged to address new challenges posed by the emergence of the digital economy.

Liability under the CPA arises when there is 'deficiency in service' or 'defect in goods' or occurrence of 'unfair trade practice'[53]. Furthermore, the CPA defines "*consumer as any person who buys any good; or hires or avails any services for a consideration which has been paid or promised or partly paid and partly promised…".*[54]This means that:

- The CPA explicitly excludes e-commerce platforms which provide services free of charge; to put it differently the CPA is not applicable when consumers provide their personal data in exchange of goods or services;
- Importantly, if actual sales are taking place on the electronic or digital network, the users/buyer will be deemed 'consumers' under the CPA and its provisions will apply to the sale of products (and consequently the 'seller' of a product shall be deemed liable).

It is important to note that the extant FDI Policy distinguishes between a market-place model – wherein an e-commerce entity acts merely as a facilitator between buyers and sellers; and an inventory-based model – where an e-commerce entity directly owns goods or services, and sells directly to consumers. Furthermore, the FDI Policy on e-commerce states that consumer satisfaction, and any warranty/ guarantee of goods and services sold will be the responsibility of the seller.[55] In this regard, the FDI Policy rightly recognises that e-commerce entities following a market-place model are only intermediaries, and the final liability for consumer protection related issues rests with a seller.

---

[51] Objective 15 of the National Policy on Information Technology, 2012, available at http://meity.gov.in/writereaddata/files/National_20IT_20Policyt%20_20.pdf

[52] Department of Electronics and Information Technology, 'Policy on Adoption of Open Source Software for Government of India'; available at http://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf

[53] Section 2 (c) of the CPA, 1986; available at http://ncdrc.nic.in/bare_acts/Consumer%20Protection%20Act-1986.html

[54] Section 2 (d) of the CPA, 1986

[55] Para 5.2.15.2.4 (vi) of the FDI Policy

At this juncture, it is important to revisit the existing Information Technology Act, 2000 (IT Act) which is based on the United Nations Commission on International Trade Law (UNCITRAL) model law on e-commerce. The IT Act defines an intermediary as *'any person who on behalf of another person receives, stores or transmits that record or provides any services with respect to the record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market places, and cyber cafes.'*[56]

Furthermore, the present legal position in India is that online marketplaces which offer hosting services are exempted from liability for the information, data, or communication hosted by them[57]. Similar safe-harbour provisions for intermediaries/marketplaces are found in other jurisdictions as well. For instance, under the EU e-commerce Directive, intermediaries which offer hosting services are exempted from liability if they do not have control or knowledge over the product hosted by them.[58]

The Policy's emphasis on information disclosure requirements is welcome. In particular, the Draft Policy proposes to mandate marketplaces to disclose information related to – (a) prices of goods or services sold in India in INR; (b) details of seller(s) including name, address, and contact details; and (c) purpose and use of data collection. It is important to note that the recently adopted Legal Metrology (Packaged Commodities) (Amendment) Rules, 2017 already impose such information disclosure requirement on e-commerce entities.[59] Therefore, the need for incorporating such information disclosure related provisions in the Draft Policy remains unclear.

Notably, with respect to digital content like video and images, the issue of consumer protection becomes more complex. In the context of digital content, issues related to consumer redressal can include a lack of clarity on who is liable in the event of a problem, particularly if multiple providers are involved. In this scenario consumers might not always be able to determine whether the problem originates with the content itself, the platform on which it was purchased or subscribed to (e.g. an app store, software vendor's platform, or streaming service), the device on which the digital content product is accessed, or the service that enables access to the product (i.e. the ISP).[60]

In such circumstances, information disclosure by e-commerce entities plays a vital role in improving consumer awareness towards the recourse available to them. Under the EU Consumer Rights Directive, businesses concluding "off-premises" and "distance" contracts are required to disclose information like details about the goods or services, details about the sellers, payment and delivery details, and consumer redressal options.[61]

---

[56] Section 2(w) of the IT Act, 2000
[57] Section 79 of the IT Act, 2000
[58] See Article 14 of the EU E-Commerce Directive, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN
[59] https://consumeraffairs.nic.in/acts-and-rules/legal-metrology/lmpc-amendment-rules-2017
[60] Organisation for Economic Co-operation and Development (OECD), 'Toolkit for protecting digital consumers'; available at https://www.oecd.org/sti/consumer/toolkit-for-protecting-digital-consumers.pdf
[61] Article 6 of the EU – Consumer Rights Directive, 2011; available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&from=EN

A similar approach has been adopted in other jurisdictions as well, where entities are encouraged (rather than mandated) to provide similar information. For instance, Australia's Guidelines for e-commerce provides that e-commerce business provide relevant information to the consumers.[62]

Nonetheless, to ensure that adequate safeguards are available for consumers purchasing goods or services from an e-commerce marketplace, such entities can be encouraged to adopt self-regulatory measures, which could include –

- ***Setting rules regarding quality of goods or services offered by the seller;***
- ***Blacklisting sellers who breach established rules;***
- ***Information disclosure regarding the seller's name, e-mail address, and physical address of the seller;***
- ***A robust internal dispute settlement mechanism.***

PRICING CONTROLS ON ADVERTISEMENT: We note that the Draft Policy proposes to regulate advertising charges in e-commerce, especially for small enterprises and start-ups, through pricing controls. Here it is expedient for DPIIT to keep in mind that the aim of market regulations/regulatory interventions is to prevent market failure, foster competition in the market, and promote consumer interest. In 2006, India's Planning Commission released a wide-ranging consultation paper exploring issues and the way forward for India's overall approach to regulation. It proposed a broad policy approach to guide future regulatory reform wherein regulations are seen as a state mechanism which primarily address market failure or equity concerns by providing rules that direct social and individual action. The Planning Commission's findings highlighted that an uneven approach to regulations has often led to unnecessary, inadequate, and expensive reform. Conversely, **the Draft Policy fails to identify specific market failures which necessitates the need for introducing pricing controls.**

It is important to note that most digital businesses provide their services free of cost to end-users, while relying on advertising revenue for scaling up their businesses. The proposal to impose pricing controls on advertising can therefore, adversely impact business models of digital businesses.

The legal validity of such a proposal also appears tenuous. It is a settled legal principle that freedom of speech and expression enshrined under Article 19(1)(a) of the Indian Constitution includes the 'right to commercial speech', and the 'right to circulation'.

The aspect of 'commercial speech' under Article 19(1)(a) has been recognised by the Supreme Court in *Tata Press Limited v. Mahanagar Telephone Nigam Limited*[63], wherein the Court held that "*advertising which is no more than a commercial transaction, is nonetheless dissemination of information regarding the product-advertised. Public at large is benefitted by the information made available through the advertisement. In a democratic economy free flow of commercial information is indispensable.*"

Furthermore, with respect to 'right to circulation', the Supreme Court of India *in Sakal Papers v. Union of India*[64] held that Article 19(1)(a) includes freedom to publish, disseminate, and circulate as

---

[62] The Australian Guidelines for e-commerce, 2006; available at http://archive.treasury.gov.au/documents/1083/PDF/australian_guidelines_for_electronic_commerce.pdf

[63] Tata Press Limited v. Mahanagar Telephone Nigam Limited, 1995 AIR 2438; available at https://indiankanoon.org/doc/752455/

[64] Sakal Paper (P) Ltd. v. Union of India, 1962 AIR 305; available at https://indiankanoon.org/doc/243002/

well. Specifically, while striking down the price control regulations for news-papers the Court held that:

> *"the right of freedom of speech cannot be taken away with the object of placing restrictions on the business activities of a citizen. Freedom of speech can be restricted only in the interests of the security of the State, friendly relations with foreign State, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence. It cannot, like the freedom to carry on business, be curtailed in the interest of the general public."*

Thus, the present proposal to regulate advertising charges can severely impact circulation of online advertisements. Notably, the advertisement revenue of e-commerce service would primarily depend on consumer-reach. Hence, the deeper the reach in terms of number of users, the larger would be advertisement revenue. Imposing pricing regulations can bring down advertising revenue, consequently forcing such platforms either to pass on the cost to end-users. Passing on the cost to end-user's can adversely affect the reach of the platform, leading to the creation of a vicious cycle, ultimately curtailing growth or quality of service of a service. The rationale behind the present proposal appears to be (presumed) presence of unfair competition. However, curtailing freedom of speech and expression available under Article 19(1)(a) on such grounds runs contrary to established jurisprudence.

IPR ISSUES:

The Draft Policy proposes several strategies to address issues related to piracy, specifically in relation to counterfeit products. While the proposals are well intentioned, it is important to note that proactive monitoring obligations are envisioned to be applicable on all e-commerce marketplaces, regardless of the nature of their operations. As such, e-commerce marketplaces in India act as intermediaries, and are therefore, exempted from liability for the information, data, or communication hosted by them if they follow requisite due diligence.[65] Further, generally e-commerce marketplaces do not exert control or own the goods sold on their platform.

In this regard, a more nuanced approach regarding affixing liability of intermediaries is required. In 2015, the Supreme Court in *Shreya Singhal* vs. *Union of India*[66] on the issue of online speech and intermediary liability, held 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. Similarly, in 2017, the Delhi High Court in the case of *Kent RO Systems Ltd. & Anr.* vs. *Amit Kotak & Ors*,[67] the Delhi High Court had held that the issue of whether an intellectual property right has been infringed by a user on an intermediary platform is not to be determined by the platforms themselves, as per the IT Act. This case also arose in the context of an e-commerce platform being requested to remove IP-infringing content. The court was clear on the fact that such a platform is simply not equipped to determine what is essentially a question of law.

However, more recently in 2018, the Delhi High Court in *Christian Louboutin vs Nakul Bajaj*[68] has adopted a more nuanced approach, illustrating the evolving nature of legal jurisprudence in India

---

[65] Section 79 (3) of the Information Technology Act, 2000 r/w Information Technology (Intermediary guidelines) Rules, 2011.
[66] (2013) 12 SCC 73.
[67] CS (COMM) 1655/2016.
[68] CS (COMM) 344/2018

around the regulation of intermediaries. The Delhi High Court has held that the liability of an intermediary could be determined on the basis of the role it plays while providing its service i.e. whether it was 'active' or 'passive'. The degree or requirement of compliance will be therefore higher in case of an intermediary having active participation in contrast to an intermediary having passive participation.

The Delhi High Court, in the aforementioned case, took into account several broad factors - such as, the platform's control over the products being sold, platform's role in facilitating sale and identifying sellers - to delineate if the marketplace in question is an 'active participant'. Specifically, the Court noted that:

> *"While the so-called safe harbour provisions for intermediaries are meant for promoting genuine businesses which are inactive intermediaries, and not to harass intermediaries in any way, the obligation to observe due diligence, coupled with the intermediary guidelines which provides specifically that such due diligence also requires that the information which is hosted does not violate IP rights, shows that e-commerce platforms which actively conspire, abet or aid, or induce commission of unlawful acts on their website cannot go scot free".*

While general monitoring obligations provided in the Draft Policy requiring all marketplaces to undertake proactive takedown and registration/concurrence with IPR owners may be infeasible, intermediaries could be classified as active or passive, through a thorough ex-ante determination by government under the provisions of the IT Act. In this context, DPIIT must revisit the strategy in the Draft Policy. We also submit that DPIIT should aim to harmonise the present Draft Policy with the National IPR Policy, 2016[69] which, inter alia, calls for addressing issues related to online piracy through technology-based measures.

INFANT INDUSTRY: The Draft Policy proposes to grant 'infant industry' status to small businesses and start-ups operating in the digital ecosystem. However, the Draft fails to clarify the intent and objective of granting infant industry status. Generally, such measures are adopted to protect local markets for enabling development of a specific industry.

We note that the existing WTO framework provides WTO Contracting Party with the flexibility to adopt WTO-inconsistent measures to promote domestic industry. Specifically, Article XVIII of GATT allows developing economies to impose quotas or increase tariffs above bindings, with the intent to promote a particular and new industry (commonly referred to as infant industries).[70] However, such measures are subject to procedural safeguards including mandatory notifications, besides mandatory consultations and negotiations with WTO Member States.[71] Presence of such onerous procedural safeguards onerous have meant that this flexibility has rarely been invoked by WTO Members.[72]

---

[69] Ministry of Commerce and Industry, National Intellectual Property Rights Policy, 2016; available at http://cmai.asia/pdf/National_IPR_Policy_12.05.2016.pdf

[70] GATT Article XVIII - Governmental Assistance to Economic Development; available at https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art18_gatt47.pdf

[71] See GATT Article XVIII: C

[72] WTO, World Trade Report, 2014; available at https://www.wto.org/english/res_e/booksp_e/wtr14-2f_e.pdf

Furthermore, if infant industry protection is to be granted on grounds of market imperfections and economies of scale (which appears to be the case in the present Draft), it is recommended that a sunset clause is attached to such measures[73].

The lack of a definitive timeline for granting economic protections can often lead to unintended consequences on competitiveness of local industry. One popular example of the unintended consequences of granting blanket protections to local industry is well-documented in the case of Brazil, which granted infant industry status to its computer (manufacturing) industry in 1977.[74] While, local industry showed initial growth potential, the technological gap between the computer industry in Brazil and the rest of the world widened, reducing the comparative advantage of local firms.

CONCLUSION

The Indian Government should adopt a principles-based approach instead of detailing prescriptive strategies. For instance, the U.S.[75] has listed out 24 high-level principles in its 'Digital 2 Dozen' document which guides the country's position in international trade negotiations on digital trade. A similar approach has also been adopted by Australia[76]. Further, towards facilitating growth of the digital economy, the government can explore multi-stakeholder forums, including representatives from across digital value chains – as recommended by the MeitY[77]; instead of the proposed one size fits all approach. Such forums can provide informed inputs to evolving a suitable digital economy strategy for the 21st century.

[73] WTO Economic Research and Statistics Division, Special and Differential Treatment in the WTO: Why, When and How?; WTO Staff Working Paper No. ERSD-2004-03

[74] Eduardo Luzio and Shane Greenstein, Measuring the performance of a protected Infant Industry, *The Review of Economics and Statistics* Vol. 77, No. 4 (Nov., 1995), pp. 622-633; available at https://www.jstor.org/stable/2109811?seq=1#page_scan_tab_contents

[75] The Digital 2 Dozen; available at https://ustr.gov/sites/default/files/Digital-2-Dozen-Updated.pdf

[76] E-Commerce and Digital Trade, Department of Foreign Affairs and Trade, Australian Government; available at https://dfat.gov.au/trade/services-and-digital-trade/pages/e-commerce-and-digital-trade.aspx

[77] Ministry of Electronics and Information Technology, India's Trillion-Dollar Digital Opportunity, February, 2019; available at https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf