K-9, Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
(tel): +91-11-43587126
www.sflc.in

To,
Shri Ramesh Abhishek
Secretary,
Department for Promotion of Industry and Internal Trade

March 29, 2019

[*Via electronic distribution*]

Subject: Comments on "Draft National E-commerce Policy - India's Data for India's Development "

Sir/ Madam,

SFLC.in is a New Delhi based not-for-profit organization that brings together lawyers, policy analysts, technologists and students to protect freedom in the digital world. We promote innovation and open access to knowledge by helping developers make great Free and Open Source Software (FOSS), protect digital civil liberties by providing pro-bono legal advice, and help policymakers make informed and just decisions with the use and adoption of technology.

We hope that the current submission proves useful.

Our submission is in line with the legal principles of our country and existing case laws.

Please feel free to contact us for any clarification or further information.

Biju K. Nair
Executive Director
SFLC.in

Executive Summary

On 23rd February, 2019, the Department for Promotion of Industry and Internal Trade ("the DPIIT") released the Draft National E-Commerce Policy ("the Draft Policy") with the objective to help stakeholders fully benefit from opportunities arising from the progressive digitization of the domestic digital economy and establish a level playing field for all stakeholders in the digital economy.

Though, titled as the 'National E-Commerce Policy' the document addresses a wide range of subjects, such as data protection and ownership, cross-border data flow, foreign investment, tax, competition issues, intellectual property ("IP") and intermediary liability, among other things. These issues affect a number of stakeholders and industries in addition to e-commerce websites and their consumers. The Draft Policy uses the words e-commerce players, intermediaries, social media, search engines, almost interchangeably.[1]

One of the main concerns with the Draft Policy is that DPIIT has gone beyond its mandate to make policy recommendations on subjects like data ownership/ protection, cross-border data flow, intermediary liability, taxation, competition and consumer protection. These topics fall under different ministries/ departments of the government such as the Ministry of Electronics and Information Technology ("MeitY") and the Ministry of Consumer Affairs, Food and Public Distribution.[2] Nowhere does the policy document make it clear that these ministries and their respective offices were consulted while arriving at the recommendations. Moreover, public consultations have already taken place under the aegis of MeitY on the areas of data protection and intermediary liability. The DPIIT is overstepping its jurisdiction and has issued recommendations which are not in line with existing statutes and their jurisprudence.

There has been a clamour for pushing data localisation and requirements of establishing an Indian office in recent tech-policy documents in India. Triggered by the Reserve Bank of India's notification[3] mandating hard localisation for all payments related data in India, we've seen data localisation requirements in the Draft Personal Data Protection Bill, 2018[4] ("the Draft Data Protection Bill") and now the draft e-commerce policy. The intended reasons for data localisation - security of data, local job creation, law enforcement access, creating a level playing field etc. are not backed by evidence. Data localisation norms may increase security risks and negatively impact the global and open nature of the Internet, instead of leading to job creation.

---

[1] The document makes it clear that terms like e-commerce and digital economy have been used interchangeably according to context. Pg. 9 of Draft National e-Commerce Policy.

[2] As per the Government of India (Allocation of Business) Rules, 1961, available here - https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_1800.pdf.

[3] The RBI notification on 'Storage of Payment System Data' is available here - https://rbidocs.rbi.org.in/rdocs/notification/PDFs/153PAYMENTEC233862ECC4424893C558DB75B3E2BC.PDF.

[4] The Draft Personal Data Protectin Bill, 2018, is available here - https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf.

In the Supreme Court's judgment in *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors.*[5] ("the Puttaswamy judgment"), it was made clear that individuals have autonomy over their personal data and that such privacy is a fundamental right as per Article 21 of the Constitution of India. Though the Draft Policy recognizes this right, it builds on this argument to contradict itself by stating that the collective data of Indians should be treated like a natural resource comparable to oil and the government holds such data in trust, to which rights could be permitted. The Puttaswamy judgment lays down certain tests for an encroachment on privacy by the State. Any such encroachment on the fundamental right to privacy must be: (a) backed by law; (b) necessary and proportionate; and (c) have procedural safeguards. The Draft Policy does not explain how these three metrics are satisfied before suggesting that data of Indians is held in trust by the government to which they can permit further rights.

The Draft Policy also touches upon intermediary liability and the protection of IP rights on intermediary platforms. This is a subject covered under the IT Act and various IP laws such as the Trade Marks Act, 1999, the Copyright Act, 1957, the Designs Act, 2000, among others. There is an evolving jurisprudence on the subject of intermediary platforms (their liability) and IP rights which the Draft Policy borrows from, but then as with other things, it builds its own principles beyond court mandated fundamentals. The DPIIT has ignored the decisions of the Delhi High Court in *Myspace v. Super Cassettes Industries*[6] ("Myspace"), which held that intermediaries cannot be expected to police all content on their platforms for infringing material; and *Kapil Wadhwa v. Samsung Electronics*[7], which recognized the right to re-sell after legitimate purchase of a trade mark protected product. Questions of content liability on social media and the 'genuineness of information' on such platforms is not the domain of the DPIIT and this debate has recently been a part of a public consultation initiated by MeitY on the Draft Intermediaries Guidelines (Amendment) Rules, 2018 ("the Draft Intermediaries Guidelines")[8]. It has not been made clear by the DPIIT whether MeitY was consulted on this subject before making such recommendations.

The tech-policy field in India has seen numerous developments in the recent past, the key ones being the introduction of the Draft Data Protection Bill, the Draft Intermediaries Guidelines, TRAI's consultation on the regulation of OTTs[9], and the Draft National E-commerce Policy. A common theme among all these policy documents have been creation of a level-playing field for domestic businesses and need felt for regulating online businesses. We believe that any policy affecting the technology sector should be released for public consultation with an adequate opportunity to provide counter comments. As these issues are inter-disciplinary and affect a wide range of stakeholders, sufficient time should be afforded to provide comments. Ministries and departments must restrict their policy recommendations to their respective mandates and must

[5] WP (Civil) No. 494 of 2012, available at https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.
[6] MySpace v. Super Cassettes Industries [236 (2017) DLT 478].
[7] Kapil Wadhwa v. Samsung Electronics 194 (2012) DLT 23.
[8] Draft Intermediaries Guidelines (Amendment) Rules, 2018, available at - https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.
[9] Consultation PaperonRegulatory Framework for Over-The-Top(OTT) communication Services, available here - https://main.trai.gov.in/sites/default/files/CPOTT12112018.pdf.

consult each other on issues of inter-departmental consideration, as per the Allocation of Business and Transaction of Business Rules, 1961.[10]

As the Draft Policy covers a gamut of subjects, we have provided our comments and recommendations in a thematic manner.

Jurisdiction of the DPIIT

The Draft Policy touches upon subjects such as data protection and ownership, cross-border data flow, competition, intermediary liability, tax and consumer protection. These issues are beyond the mandate and jurisdiction of the DPIIT. The Constitution of India empowers the President to allocate various functions of the Government of India through the Allocation of Business Rules, 1961[11] ("the Allocation of Business Rules).[12] On matters related to e-commerce, the Allocation of Business Rules empowers the DPIIT to issue policy in consultation with MeitY. The Draft Policy does not state whether it was drafted after consulting MeitY on the relevant issues. On policy matters related to information technology and the Internet, which the Draft Policy addresses in comprehensive detail, only MeitY has jurisdiction and not DPIIT.

Rule 3 of the Transaction of Business Rules, 1961[13] makes it clear that the business allotted to a department under the Allocation of Business Rules shall be disposed off only under the minister in charge of such department. Rule 4 of the Transaction of Business Rules states that in matters of inter-departmental consultations (such as in this case between DPIIT and MeitY on matters of e-commerce) no 'decision' or 'order' can be issued without the concurrence of all those departments whose business gets affected by such a decision. Therefore, according to the Allocation of Business and Transaction of Business Rules of the Government of India, it becomes imperative on DPIIT to consult MeitY when commenting and issuing a draft policy on the subject matters covered under MeitY's mandate.

In the recent past, MeitY has issued relevant policy documents such as the Draft Data Protection Bill accompanied with the Justice B.N. Srikrishna Committee Report[14] ("the Srikrishna Committee Report"), and the Draft Intermediaries Guidelines. These documents cover issues related to data protection, cross-border data flow and intermediary liability in detail. A policy comment on these subjects right after public consultations with MeitY have concluded on these matters, especially

[10] The Government of India (Allocation of Business) and (Transaction of Business) Rules, 1961, are available here - https://cabsec.gov.in/writereaddata/allocationbusinessrule/completeaobrules/english/1_Upload_1800.pdf and https://cabsec.gov.in/writereaddata/transactionofbusinessrulescomplete/completeaobrules/english/1_Upload_1816.pdf.
[11] Id. Note 2.
[12] Article 77 of the Constitution of India empowers the President to issue rules for the allocation of business of the Government of India between various ministries and departments.
[13] The Government of India (Transaction of Business) Rules, 1961, can be downloaded here - https://cabsec.gov.in/writereaddata/transactionofbusinessrulescomplete/completeaobrules/english/1_Upload_1816.pdf.
[14] A Free and Fair Digital Economy Protecting Privacy, Empowering Indians - Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, available here - https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

when DPIIT has made recommendations parallel and in excess of suggestions made by MeitY, causes ambiguity on the stance of the government on these issues.

Similarly, issues relating to competition law (which are covered in the Competition Act, 2002 and the nodal government agency for which is the Competition Commission of India) are included in the functions of the Ministry of Corporate Affairs as per the Allocation of Business Rules, and not DPIIT.

The DPIIT has gone beyond its remit and functions as listed in the Allocation of Business Rules when commenting on data protection and ownership, intermediary liability, taxation and consumer protection[15].

We recommend that DPIIT must restrict its comments to matters falling under its functions i.e. e-commerce (after consulting with MeitY), foreign investment and IP rights and it should re-draft and re-consider the Draft Policy considering the limitations of its mandate. Any draft policy document issued by DPIIT must be made public and a process of inviting comments and counter-comments must be initiated maintaining complete transparency.

Data Ownership and Sovereignty

The Draft Policy discusses data ownership and sovereignty in fair detail. It likens data to oil and states that as a natural resource, a country has sovereign rights over its data. In Chapter I of the Draft Policy, the DPIIT acknowledges an individual's right to her data, which cannot be used without the express consent of the individual to whom it belongs. Though, this is line with the *Puttaswamy* judgment (which recognized the autonomy of an individual on his/her data), the policy document goes on to compare group data to a collective property of the group. Using this collective property analogy, the policy concludes that the data of a country should be best thought of as a collective resource and a national asset, which the government holds in trust, but rights to which could be permitted. The Draft Policy also bars business entities from sharing the sensitive data of Indians, which is stored abroad, with third parties, 'even after customer consent'.

These are fresh principles propounded by the DPIIT on data ownership, which are not in line with either the *Puttaswamy* judgment or the Srikrishna Committee Report. The Supreme Court recognized the individual's autonomy over her data and stated that unauthorized use of personal information will result in infringement of the right to privacy.[16] The Supreme Court in *Puttaswamy*, laid down three-tests for encroachment upon privacy rights of individuals by the State - a) the action must be sanctioned by law; b) it must be necessary for a legitimate state aim and interference must be

[15] The Draft Policy comments on issues of taxation as well, which fall under the mandate of the Ministry of Finance, Department of Revenue, as per the Allocation of Business Rules and not the DPIIT. Similarly matters of consumer affairs and protection fall under the Ministry of Consumer Affairs, Food and Public Distribution.

[16] Para. 81 of Justice Nariman's judgment in KS Puttaswamy v. Union of India states that *"Informational privacy which does not deal with a person's body but deals with a person's mind, and therefore recognizes that an individual may have control over the dissemination of material that is personal to him. Unauthorised use of such information may, therefore lead to infringement of this right."*

proportionate to its need; and c) there must be procedural guarantees against the abuse of such interference. Any suggestion made by the DPIIT which dilutes the data privacy rights of individuals will have to pass these tests as laid down in *Puttaswamy*. Similarly, the Srikrishna Committee Report also recognized the importance of protecting the autonomy of an individual as critical, not just for her own rights but constitutive of the free and fair digital economy.[17] This ideology of the country's data being considered as a collective resource to which government may permit rights is not in consonance with the current law of the land as propounded in *Puttaswamy*.

One of the aims of the Draft Policy is to enable the sharing of anonymised community data like - data collected by IoT devices installed in public spaces like traffic signals and automated entry gates. At the same time, the policy recognizes that even after data is anonymized, the interests of the individual cannot be separated from it.

Even the Srikrishna Committee Report acknowledges that it is possible to identify individuals from data sets which are seemingly anonymised.[18] The Data Protection Bill, authorises the proposed Data Protection Authority of India to issue appropriate standards for the anonymisation of data so that it cannot be re-identified. The Draft Policy does not establish any standards for anonymisation of community data and it only places responsibility on a 'data authority' for the implementation of anonymised community data.

We recommend that the data aspects of the Draft Policy should be removed as these are covered comprehensively by the Puttaswamy judgment, the Srikrishna Committee Report and the Draft Data Protection Bill.

Restriction of Cross-Border Data Flow

The policy calls data the new oil and seeks to exploit the data of Indians for the country's growth and development. It proposes creating legal and technological restrictions on cross-border data flow from specified sources. The sources include (a) data collected by IoT devices installed in public space; and (b) data generated by users in India by various sources, including e-commerce platforms, social media, search engines etc. Both (a) and (b) reveal that the e-commerce policy intends to regulate data from sources that are beyond the scope of DPIIT.

Localisation of such a broad range of data creates a situation of 'keeping all eggs in one basket' and makes user data more vulnerable to hacks. Given India's near unqualified communication surveillance capabilities bolstered by lack of transparency and absence of independent oversight, centralising data storage within one jurisdiction may even facilitate greater surveillance from within.

The Draft Policy maintains that placing restrictions on cross-border data flow is vital for reducing entry barriers for second movers. The intention is to enable start-ups and small business to

[17] A Free and Fair Digital Economy, Protecting Privacy, Empowering Indians, Committee of Experts under the Chairmanship of B.N. Srikrishna, Pg No. 9
[18] Id. Pg. No. 28

successfully compete with established first movers in the data driven ecosystem. The policy downplays the importance of the IT/ITeS sector in India by stating that "domestic technology companies would be merely processing outsourced data work".

Restrictions on cross-border data flows such as data localisation/ mirroring are counterproductive in the present technological reality which points to a rise in outsourcing services, ITeS, disruptive utilities like cloud computing and global social media communication exchange, among others. Overarching government regulations would stifle innovation in the IT sector which contributes more than 60% to India's GDP. A study on economic losses caused by data localisation shows negative impact on GDP in all cases such as -1.1% in China and -1.7% in Vietnam. It adds that losses in India would be 0.1% of GDP for sectoral implementation of localisation.[19] A blanket localisation would raise the economic losses by eight times[20].

An analysis of data localization laws in Russia shows loss in trade flows, businesses, manufacturing sector and more importantly small IT businesses.[21] Data retention costs would be significant as it'll include initial capital expenditures, maintenance of a required security level, routine hardware replacement, electricity costs etc.[22] Moreover, unlike France and Australia, there is no reference to subsidisation and tax breaks to compensate for the cost burden of localisation and mirroring.

The Draft Policy also dismisses the benefits of Internet and goes on to say that expected gains of equal market access and opportunities for growth offered by the Internet have not reached small businesses. These have largely accrued to the first movers. Contrary to these claims, research shows that gains from free and open Internet has contributed vastly to India's growth story. Internet's contribution to India's GDP has been at about 5% with Internet enabled applications contributing a minimum of USD 20.4 billion in 2015-16; this share is expected to grow to 15% by 2020 with a whopping USD 270.9 billion coming from the App economy.[23] Any restrictions on cross border flow will prove detrimental to the future economic growth of the country.

The Draft Policy also argues that it is vital that we retain control of data to ensure job creation within India. The studies on the contrary have shown that in India, loss per worker would be nearly 11% of the average monthly salary if data retention requirements are imposed.[24] Besides, considerable loss in domestic investment of 1.4% to 1.9% is also expected in India.[25] This could reduce competition in Indian IT industry, especially when the government is pushing to promote

[19] The Costs of Data Localisation: A Friendly Fire on Economic Recovery, Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, & Bert Verschelde, ECIPE Occasional Paper No. 03/2014
[20] Id.
[21] Could the recently enacted data localisation requirements in Russia backfire, Iva Mihaylova, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2629533
[22] Id.
[23] Estimating the Value of New Generation Internet Based Applications in India, July 2017, Indian Council for Research on International Economic Relations ,ICRIER, http://icrier.org/pdf/Estimating_eValue_of_Internet%20Based%20Applications.pdf
[24] The Costs of Data Localisation: Friendly Fire on Economic Recovery(ECIPE), available at http://ecipe.org/publications/dataloc/
[25] Id.

ease of doing business. Data localisation will impose higher compliance burdens, and cost overheads especially on small businesses and startups that rely mostly on foreign servers for processing their data. These will eventually have to import hardware from abroad.

While recommending a restriction on the cross-border flow of data generated by users in India, the Draft Policy has not taken into consideration the full list of sources from which such cross-border flow is meant to be restricted. The use of blanket and vague terms such as 'various sources', 'social media' and 'e-commerce platforms' is likely to have a negative impact on the digital rights of people. Restricting the flow of social media data, for example, would have repercussions beyond the monetization of the data itself. It would restrict the ability of people to communicate across borders.

The Internet is border-less by design. Forcing geographical borders onto the Internet would pose unnecessary impediments to freedom and innovation without any apparent benefit for the rights of the people. If every country were to enforce data localisation requirements, then every entity that wanted to provide a service across the world would need to store and process the data of every person within the boundaries of the specific country that they belong to. Such data localisation would also prevent users from accessing their own data when they are travelling through another country. The only beneficiaries in such a situation would be large corporations that would face less competition when deploying services across the globe as compared to the small business that would not be able to afford similar costs.

Such attempts would result in the creation of an Indian Internet that will be walled away from the rest of the Internet.

The Draft Policy stipulates broad strategies to facilitate local storage of data such as data centres, server farms, towers, tower stations, equipment, optical wires, signal transceivers and antennae.

Data centres are highly energy intensive and specialised cooling systems will be required in data centres to keep their temperatures at optimal level. Data centres are presently responsible for 2% of greenhouse gas emissions, which is at the same level as the aviation sector.[26] These financial costs, how much cooling is required and the resultant greenhouse gas emissions would be even higher in a tropical country like India.

Before entailing massive data storage projects, due regard must be paid to these facts and a detailed feasibility assessment of these will have to be done.

We recommend that suggestions to introduce broad data localisation requirements should be removed from the Draft Policy as this issue is under consideration in the Draft Data Protection Bill. Sectoral regulators like the RBI have their own mandates on data localisation and DPIIT's suggestion will create a parallel requirement adding to ambiguity.

[26] The Guardian: How viral cat videos are warming the planet, available at https://www.theguardian.com/environment/2015/sep/25/server-data-centre-emissions-air-travel-web-google-facebook-greenhouse-gas

Disclosure of Source Code

The Draft Policy states that it's important for the Government to reserve its right to seek disclosure of source code and algorithms in order to explain the decisions of Artificial Intelligence systems.

Source code and algorithms fall within the ambit of the Copyright Act, 1957 ("the Copyright Act"). Under the Copyright Act, a copyright owner may choose to grant a license or assign the copyright to another party. While the Copyright Act allows for compulsory licensing in certain situations, it does not allow the Government to reserve any right to seek disclosure of a copyrighted work.

Selective disclosure to only the Government could lead to hoarding of vulnerabilities. Such disclosures would raise concerns among businesses and end users that rely on information technology products, leading to lower adoption of solutions/ products/ services created or made available in India. This would lead to lower foreign investment in the information technology sector in India.

Disclosure of source code to the general public under an open source license allows others to build upon the work and it allows security researchers to find vulnerabilities. However, such disclosures are voluntarily made under appropriate licenses that operate under copyright law.

We recommend removing any requirement for forced disclosure of source code, except in the following circumstances: (a) If a product/ solution/ service is created with funds provided by the public through the State, its source code should be made publicly available under a Free and Open Source (FOSS) license; (b) Source code disclosure should be mandatory for acquisition of any product/ solution/ service by the State.

Counterfeiting and Piracy on E-commerce Platforms (Intermediary Liability and IP)

To restrict the exchange of counterfeit and pirated goods and services on e-commerce platforms, the Draft Policy recommends various measures to be undertaken by platforms. The policy lists down different requirements for products protected by trademark and separate strategies for the protection of content covered by copyright. A few decisions by the Delhi High Court have laid down the jurisprudence around take down of IP protected content from various Internet platforms, namely - *Myspace v. Super Cassettes Industries*[27]; *Kent RO v. Amit Kotak*[28] ("Kent RO"); and *Christian Louboutin v. Nakul Bajaj*[29]. Though, most of the measures suggested by the Draft Policy are in accordance with the court's jurisprudence, some recommendations go above and beyond.

[27] Id. Note 6.
[28] Kent R O Ltd. v. Amit Kotak [2017 (69) PTC 551 (Del)]
[29] Christian Louboutin SAS v. Nakul Bajaj and Ors. (Civil Suit No. 344/2018)

For sale of counterfeit products protected under trademark law

Paragraph 3.11 of the Draft Policy makes a recommendation that whenever a trademark protected product is uploaded on an online platform, the portal shall notify the trademark owner. Such a requirement must not lead to pre-screening/ filtration systems which results in constant monitoring of all products being uploaded on the online platforms, as this will be against the decisions in *Myspace and Kent RO*, which clearly lay down that intermediary platforms must not be required to constantly monitor their platforms for infringing material.[30]

Paragraph 3.12 enables trademark owners to not have their products listed on a particular platforms without their prior concurrence, if so desired. Apart from these requirement not leading to pre-screening/ filtration systems, prior concurrence of trademark owners each and every time a product having their mark gets uploaded will negatively affect the right to re-sell or the sale of second hand goods on e-commerce platforms. This is also supported by the principle of domestic/ international exhaustion, according to which, once a trademark owner legitimately sells its product, its exclusive right to sell such a product gets exhausted and it cannot be reignited. The principle of exhaustion has been recognized under Section 30(3) of the Trade Marks Act, 1999 and by the Delhi High Court in its landmark judgment - *Kapil Wadhwa v. Samsung Electronics*[31].

In paragraph 3.16, the Draft Policy seeks to re-install a notice and takedown regime, wherein platforms will have to takedown product listings, if a customer complains to it about the genuineness of a product. This is in contradiction to the established jurisprudence as recognised by the Delhi High Court in *Myspace and Kent RO*, wherein, only rights owners (not any third party or customers/ consumers) may request online platforms to take down product listings which infringe their IP rights. For doing so, IP owners will be required to identify and point towards specific cases of infringement and intimate the online platform for takedown.[32]

For distribution of pirated content protected under copyright law

Paragraph 3.18 of the Draft Policy states that 'intermediaries' (instead of restricting to e-commerce platforms, the policy document uses the words intermediaries for this section, which covers a large number of stakeholders and not just e-commerce players[33]) shall put in place measures to prevent online dissemination of pirated content. Protection to copyright owners for dissemination of pirated content on online platforms is already available via takedown measures as provided under the IT Act and the Copyright Act. According to the decision of the Delhi High Court in *Myspace*, copyright owners may point to specific instances of infringement to online platforms and they will need to take it down. Intermediaries themselves cannot be tasked with identifying infringing content from legitimate content as this may have a chilling effect on free speech.[34] Thus, this recommendation for

[30] Para. 62 of Myspace and Para 30. of the Kent RO decisions.
[31] Kapil Wadhwa v. Samsung Electronics 194 (2012) DLT 23.
[32] Para. 57 of Myspace judgment and Para 35. of Kent RO judgment.
[33] The term intermediary has been defined under Section 2(1)(w) of the Information Technology Act, 2000 and it includes a number of industry players such as - telecom service providers, Internet service providers, search engines, cyber cafes etc. apart from e-commerce platforms.
[34] Para. 62 of the Myspace judgment.

intermediaries to take 'measures' for eliminating pirated content is - already covered under appropriate law, is unclear in its import, and may lead to installation of pervasive monitoring of online platforms which will be in contradiction to existing jurisprudence on the subject.

We recommend that all measures and strategies suggested by DPIIT to stop the exchange of counterfeit and pirated goods on online platforms must be in accordance with relevant provisions in existing statutes (Trade Marks Act, 1999; Copyright Act; and the IT Act) and the jurisprudence on these subjects.

Social responsibility of online platforms and social media

The Draft Policy comments on the liability of online platforms and social media on the content circulating on their platforms. The DPIIT has stated that with the growing importance of such platforms their social responsibilities also increases and content posted on such websites should not be compromised. Social media tools and other entities who post content on behalf of third parties on their platforms, are given a conditional protection under the Information IT Act for the content which is posted on their websites. As per the IT Act, such entities (intermediaries) are not required to actively monitor their websites for third party content. In a landmark judgment by the Supreme Court of India in *Shreya Singhal v. Union of India*[35], the court made it clear that online intermediaries cannot be asked to be the adjudicators of legitimate speech.

The policy uses ambiguous terms such as - 'social responsibility' and 'genuineness of information', which does not make it clear as to what is the precise responsibility of online platforms and social media applications when it comes to their liability for content on their platforms. Intermediary liability, which the Draft Policy seeks to address, has recently been the issue of discussion in a public consultation initiated by MeitY on the Draft Intermediaries Guidelines.[36]

We recommend that the DPIIT remove the portion on 'Exemption from Content Liability' from the Draft Policy as this subject i.e. online intermediary liability is covered under the IT Act and corresponding jurisprudence.

Law Enforcement Access to Data

The Draft Policy argues that due to the all pervasive nature of e-commerce and the digital economy in Indian life, access to data for maintenance of law and order has attained paramount importance. The document also recommends that 'participants of the digital economy' who process the data of Indians, must nominate a local representative who'll be responsible for the affairs of the company in India.

[35] Para. 117 of Shreya Singhal v. Union of India [AIR 2015 SC 1532]

[36] The recently concluded public consultation on the Draft Intermediaries Guidelines (Amendment) Rules, 2018 by MeitY discusses these issues in detail. For our comments on the draft rules, kindly visit - https://sflc.in/our-comments-meity-draft-intermediaries-guidelines-amendment-rules-2018

On the aspect of access to data by law enforcement agencies, existing provisions in the IT Act give sufficient powers to law enforcement agencies to gain access to data. Section 69 of the IT Act empowers the Government, both at the centre and state level to intercept, monitor and decrypt data for inter-alia, maintenance of public order and preventing the incitement and investigation of offences. Similarly, Section 69B of the IT Act empowers the Central Government to monitor and collect traffic data (including meta-data) for cyber security purposes (both provisions prescribe procedural safeguards for eliminating abuse of powers). The Draft Policy when discussing access to data by law enforcement does not refer to these provisions already contained under the IT Act.

The policy does not define the phrase - 'participants of the digital economy', while recommending that such organizations must nominate a local representative responsible for affairs of the company. This requirement doesn't make it clear as to whom does it apply to and how the presence of a local representative will enhance existing law enforcement powers of gaining access to data. In a recently concluded public consultation by MeitY on the Draft Intermediaries Guidelines, a similar recommendation was made for intermediaries having upwards of 5 million users in India.[37] If all businesses on the Internet are required to have a local representative, it will negatively affect the open nature of the Internet. Foreign not-for-profit and other smaller entities wanting to provide their services in India using the global nature of the Internet will get impacted by the local office requirement. Competition in the digital economy will reduce, eventually resulting in fewer options for consumers. Indians might lose access to services like free web-browsers, open source messaging applications and open encyclopedias if mandatory local office requirements are put in place.

We recommend that the DPIIT rely on existing provisions in law, specifically under the IT Act for access to data by law enforcement. The local office/ representative requirement should be removed, firstly for its ambiguous and negative effects and secondly, as MeitY is considering a similar requirement under law for which a public consultation was recently conducted.

Summary of Our Recommendations

- We recommend that DPIIT must restrict its comments to matters falling under its functions i.e. e-commerce (after consulting with MeitY), foreign investment and IP rights and it should re-draft and re-consider the Draft Policy considering the limitations of its mandate. Any draft policy document issued by DPIIT must be made public and a process of inviting comments and counter-comments must be initiated maintaining complete transparency.
- We recommend that the data aspects of the Draft Policy should be removed as these are covered comprehensively by the Puttaswamy judgment, the Srikrishna Committee Report and the Draft Data Protection Bill.
- We recommend that suggestions to introduce broad data localisation requirements should be removed from the Draft Policy as this issue is under consideration in the Draft Data Protection Bill. Sectoral regulators like the RBI have their own mandates on data localisation and DPIIT's suggestion will create a parallel requirement adding to ambiguity.

[37] Refer to Rule 3(7) of the Draft Intermediaries Guidelines.

- We recommend removing any requirement for forced disclosure of source code, except in the following circumstances: (a) If a product/ solution/ service is created with funds provided by the public through the State, its source code should be made publicly available under a Free and Open Source (FOSS) license; (b) Source code disclosure should be mandatory for acquisition of any product/ solution/ service by the State.
- We recommend that all measures and strategies suggested by DPIIT to stop the exchange of counterfeit and pirated goods on online platforms must be in accordance with relevant provisions in existing statutes (Trade Marks Act, 1999; Copyright Act; and the IT Act) and the jurisprudence on these subjects.
- We recommend that the DPIIT remove the portion on 'Exemption from Content Liability' from the Draft Policy as this subject i.e. online intermediary liability is covered under the IT Act and corresponding jurisprudence.
- We recommend that the DPIIT rely on existing provisions in law, specifically under the IT Act for access to data by law enforcement. The local office/ representative requirement should be removed, firstly for its ambiguous and negative effects and secondly, as MeitY is considering a similar requirement under law for which a public consultation was recently conducted.
