March 29, 2019

To,
Shri Ramesh Abhishek
Hon'ble Secretary,
Department for Promotion of Industry and Internal Trade,
Ministry of Commerce and Industry,
Government of India

Subject: Access Now comments on DPIIT's draft e-commerce policy

Dear Sir,

We write to you to submit our responses in response to consultation invited on Draft National e-Commerce Policy (Draft Policy) published by Department of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry. This letter contains Access Now's initial inputs in response to the consultation invited on Draft Policy.

Access Now is an international non-profit organisation which works to defend and extend the digital rights of users at risk globally. Through presence in 10 countries around the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also engages with its global community of nearly half a million users from over 185 countries, in addition to operating a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world. We coordinate as part of CiviCERT (Computer Incident Response Center for Civil Society) a Trusted Introducer accredited CERT. We also have special consultative status at the United Nations.[1]

In discussing the path to enable the growth of the e-commerce sector and the digital economy as a whole, the Draft Policy provides far-reaching guidance on the regulation of data. The Draft Policy would have great impact on the digital rights of Indian, especially the right to privacy, as affirmed by the seminal judgement in the matter of *Justice KS Puttaswamy (Retd.) & Anr. v. Union of India & Ors [W.P. (C) 494/2012]* by the Supreme Court in India. Below we provide our detailed feedback on the draft policy in the context of its impact on the digital rights of the people in India.

Detailed Feedback

1. **A comprehensive data protection and surveillance regime is a foundational requirement and of paramount importance**

[1] Access Now, About us, https://www.accessnow.org/about-us/

The *Puttaswamy* judgement affirmed the fundamental right to privacy in India, and further made it clear that it is incumbent on the Union Government to provide meaningful protections of this right through the enactment of a comprehensive data protection and privacy regime in India. The rights of the people of a country are an end in themselves. While the Draft Policy focuses on enabling domestic players, digital transactions, e-Governance, and the digital ecosystem at large, we believe that safeguarding and empowering the people must be the primary and foundational aim of any such policy framework.

Safeguarding the digital rights of people in a country is essential for the development of the digital economy as well. It is only on a strong foundation of respect and empowerment of the digital rights, that the digital economy would be able to develop in a manner which serves the interests of the nation and its people. We urge the DPIIT to encourage and support the Government of India to establish a comprehensive and rights respecting data protection framework; this must become a foundational goal of the Draft Policy.

The Government of India has been considering a draft data protection legislation or the Personal Data Protection Bill, 2018, drafted by an expert committee led by Justice B.N. Srikrishna. This committee process and its recommendation find only a brief mention in the Draft Policy. It is crucial that the e-commerce policy be framed to be in consonance with a national data protection framework, and have a strong focus on privacy.

It is highly discouraging that the Draft Policy, while proposing a path to leverage data for the growth of the digital economy, does not distinguish between personal data, sensitive personal data and other forms of data. This intrinsic distinction between different kinds of data is essential in protecting the rights of users, along with defining the contours of protections which cannot be broached by commercial entities and the government.

In order to secure the privacy of the people, it is necessary that they should be entitled to seven binding rights to users[2], in relation to their personal and sensitive personal data:

a. **Right to access**: user's right to obtain confirmation as well as the right to access to the data, the purpose for the processing, by whom it was processed, and more.
b. **Right to object**: user's right to restrict data processing, in case the data has been collected without their prior explicit consent
c. **Rights to erasure**: user's right to ask for erasing their data when a user opts-out of a service or application
d. **Right to rectification/ correction**: users' right to modify inaccurate or incorrect information about them

[2]. Accessible at https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf

e. **Right to information**: users' right to receive information from the companies in an understandable form, whether their data has been directly collected by the company or has been acquired from a third party. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.
f. **Right to explanation**: users' right to get information about the reason because of which their data is being processed and the possible consequences of such data processing.
g. **Right to portability**: users' right to move their personal data from one platform to other similar platforms.

2. Framing user data as a natural resource

In many instances, the Draft Policy highlights that data is a natural resource - 'data is the new oil'. Flowing from this, the Draft Policy has argued that India has sovereign rights over the data of its citizens. Further, treating data as a natural resource, the Draft Policy presents that data must be exploited for the benefits of the nation, by enabling the state to exercise power over it, and allowing the state to distribute it among Indian entities

We are concerened that this approach, and the arguments flowing from it, would be incompaitabile witht the fundamental right to privacy, as enshrined in the Constitution of India and in international human rights law. An individual's data is covered by their rights to privacy and data protection. The individual is entitled to be provided protection and privacy by the state, as well as from intrusions into their privacy or misuse of personal data by other entities in the country. Even the Srikrishna Committee, following the model of the European General Data Protection Regulation, provides in its proposed framework that the individual is the holder of the right to their data and privacy. The individual's right to privacy must be provided protections even against the state.

Given its status as an essential component of the right to privacy of an individual, data should not be reduced to only being considered a common resource or public good to be leveraged by the state. As discussed above, the primary responsibility in the context of the state, is to ensure that a rights respecting data protection framework - including one that provides adequate surveillance reform and oversight - is introduced in the country.

The Draft Policy acknowledges the elements of individual's rights regarding their dataon page 5 of the Draft Policy, wherein it states "An individual consumer/user who generates data retains ownership rights over his/her data (pp. 5-6).". The Draft Policy build on this basic ethos, and not conflate the right of the individual by extending them to be the sovereign rights of the state.

Furthermore, we are deeply concerned that the Draft Policy recommends that the natural resource of data must be exploited for "maximising growth" of the e-commerce sector. There are recommendations regarding leveraging anonymised community data for the benefit of Indian industry. We suggest exercising caution, as the exploitation of data can easily translate to the exploitation of the rights of the citizens. It is essential that the data protection framework, provide adequate protections in the form of notice, consent, data minimisation and purpose limitation among others, to ensure that growth of the e-commerce sector and the digital economy does not come at the cost of the rights of the people in India. In relation to "community data", it must be noted that even data collected at "public places" must be collected and processed within the contours of a right respecting data protection framework.

3. Cross Border Data Flows and Data Localisation

The Draft Policy in various instances refers to the need of regulating cross border data flows, imposing restrictions on such data flows, and promoting data localisation. As noted in our assessment of the data protection framework proposal of the Srikrishna committee - *Assessing India's Proposed Data Protection Framework: What The Srikrishna Committee Could Learn From Europe's Experience*, proposals for data localisation dilute India's connection to the global internet and betray a governmental interest in desiring more control over the data of Indian citizens. Such proposals may facilitate third-party abuse of personal data and infringe on users' right to privacy, as actors would know where data is located. Further, they go against the spirit and objective of a data protection and privacy legislation.

Research by scholars such as Anupam Chander provides evidence that data localisation does not provide economic benefits, and would likely have an adverse effect on the open nature of the global internet. Further, in the absence of much needed surveillance reform in India, data localisation explicitly increased overt governmental access to data and private communications of Indian residents, while not taking steps to increase oversight and checks meant to secure their privacy.

In relation to cross border data flows, it is essential that the data of the people of India is provided adequate safeguards when it crosses Indian borders. Modern data protection frameworks - particularly the EU GDPR, as well as partly in the proposals made by the Srikrishna committee - generally instead focus on putting in place an "adequacy mechanism". This involves the government and the data protection authority evaluating the data protection frameworks ofr foreign countries in order to see if they can be judged as providing adequate data protection rights and remedies to users regarding their data if it is transferred to its territory. These mechanisms promote a healthy and constructive manner of establishing international norms, while also ensuring the protection of the rights of the people of all countries involved.

Additionally, we are concerned by the problematic strategies proposed by the Draft Policy on page 16:

1. Providing *basis for sharing the data collected by IoT devices with domestic entities for use in research and development for public policy purposes*: we suggest exercising caution in providing blanket access to domestic entities. Such access must be within the contours of a rights respecting data protection framework. Criteria like research and development can be misused for the exploitation of people, included as observed in the case of the Cambridge Analytica revelations.
2. *All such data stored abroad shall not be made available to other business entities outside India or any third party, for any purpose, even with the customer consent*: Such restriction undermine user agency and choice, and if adequacy mechanism are established, as discussed above, such measures become unnecessary.

We, therefore, submit that the ecommerce policy and the DPIIT must work towards establishing rights respecting models of cross border flow of data, and withdraw proposals for data localisation.

4. Regulatory Proposals in the Draft Policy

There are certain regulatory proposals within the Draft Policy which have a direct impact on the digital rights of people in India.

a. The Draft Policy recommends establishing norms to facilitate domestic companies being able to compete with the first-mover foreign entities in the Indian market. We believe that establishing “right to data portability” would provide space for developers and competitive technology firms to compete in the market, while ensuring that the users are able to avail services which are most beneficial to them and their rights.
b. Further, there are proposals for requiring disclosure of source codes and algorithms. We believe that instead, it would be better for the Government to work on ensuring that users are given a“right to explanatio”n that they can seek from the entities using their data. The users should be entitled to understand the processing of their data and the decision making process where such data is used to make decisions about them.
c. There are proposals which require that the government must be provided access to data for maintaining law and order, regardless of the legality of the order and whether the procedure matches standards regarding necessity and proporotionatlity. Establishing norms for indiscriminate access to data by the government would undermine several of its own priorities with regards to the digital economy as well as enhanced international law enforcement cooperation. Specifically, we believe that it would inhibit the potential grant of adequacy status to India by countries with existing data protection frameworks. Such measures would also take India a step back in bilateral discussions of law enforcement access to data such as through MLAT processes, and other mechanisms such as United States’ CLOUD Act.
d. The Draft Policy discusses leveraging data collected by the government itself. It must be noted that making strides in establishing and implementing a clear open data policy for

the government would help entities leverage this data in a manner beneficial to India's policy goals, provided it is done in a way to respects individual rights to privacy and data protection.

e. Lastly, the Draft Policy discusses emphasizing liability and responsibility of intermediaries and social media platforms in ensuring the genuineness of information on their websites. This recommendation comes in the context of another recent proposal of the Ministry of Electronics and Information Technology to amend the intermediary guidelines issued under Section 79 of the Information Technology Act. As noted by an international coalition of civil society organisations and security experts, imposing prior censorship and takedown requirements, along with increased obligations regarding sharing of private information with government agencies outside of strict processes will chill the freedom of expression and right to privacy of Indian residents.

We hope our recommendations aid the Ministry in ensuring that the further development of India's e-commerce policy environment does so in a rights respecting way, helping deepen the potential of the internet to countless individuals.

We stand available to assist the Ministry for any clarification or other assistance required in this process.

Thanking you,

Yours sincerely,

Naman M. Aggarwal,
Asia Policy Associate

Raman Jit Singh Chima,
Asia Policy Director

Access Now | https://www.accessnow.org