Mozilla Headquarters
331 E Evelyn Avenue
Mountain View, CA 94041
United States of America
650.903.0800

To
The Department of Promotion of Industry and Internal Trade
Government of India
New Delhi

29 March 2019

We thank the Department of Promotion of Industry and Internal Trade for the opportunity to provide feedback on the Draft National E-Commerce Policy (hereafter, "the Policy"). We welcome the broadening of this consultation to invite suggestions from experts, stakeholders, and the general public.

Mozilla is a global community working together to build a better internet. As a mission-driven technology company, we are dedicated to promoting openness, innovation, and opportunity online. We are the creators of Firefox, an open source browser and the family of Firefox products, including Firefox Focus and Firefox Lite, as well as Pocket, used by hundreds of millions of internet users globally. Mozilla's commitment to user security and privacy is evident not just in our products but in our policies and in the open source code of our products.

In this submission below, we respond to certain key issues in the Policy, and offer analysis and recommendations based on our experience and expertise advocating for competition, security, and privacy all over the world. In particular, we offer our views on the formulation of data as a "national asset"; restrictions on storage and sharing of data; requirements to disclose source code; and access to data as a means to encourage competition.

It is the Government of India's prerogative to formulate digital policy in accordance with national priorities. The main priority area identified in the Policy is to increase the competitiveness of domestic industries at the expense of foreign companies. However, rather than viewing this as a zero-sum game, there is much for India to gain by leveraging the interconnectedness of the global digital economy.

India has already demonstrated its leadership on the global stage when it comes to internet policy. TRAI's net neutrality regulation, perhaps the strongest in the world, was heralded globally as a powerful means to ensuring competition online, taking a stand against some of the largest companies, and

protecting Indian users. At a time when US law is being widely criticized for failing to meet the privacy and competition challenges of the day, India has a unique opportunity to lead and raise the standards of data protection and competition globally.

However, some of the blunt strategies proposed in this Policy could isolate Indian companies from their global counterparts, and cause other countries to retaliate with similar measures that would be counterproductive to India's interests. The digital economy is characterized by diverse partnerships and business relationships to deliver the best services to the user at the lowest cost. This interconnectedness is especially important for small and growing businesses who depend on outsourcing a range of functions to global companies in order to keep costs sustainable and scale. Some of the measures contemplated in the Policy would limit the ability of Indian firms to partner with and leverage the best firms globally. At the same time, these measures would almost assuredly reduce foreign investment and disincentivize working with Indian firms. Ultimately, a maximalist focus on boosting domestic industry could hurt the very businesses it is meant to serve, while limiting competition, and diminishing the choices of users. These impacts would be magnified if another country were to enact a similar regime on Indian firms.

While many of the strategies proposed in the Policy focus on enabling access to data for the Indian government and businesses, ensuring the privacy and security of this data is merely noted as an afterthought. Given that India currently lacks a comprehensive data protection law and India has some of the weakest regulations around government surveillance, such permissive access to Indian entities does not adequately protect Indian users. These legal safeguards are a precondition to any credible data-focussed digital policy. As we've argued extensively to the MEITY and the Justice Srikrishna Committee, such a law has the opportunity to build on the globally high standard of data protection set by Europe, and position India as a leader in internet regulation. To this end, we urge the government to prioritize the passage of a strong data protection law, accompanied by reform of government surveillance.

Similarly, India has the opportunity for global leadership on advancing progressive competition law reform to address the challenge of concentration of power in a handful of online companies. We support a broad-based reform of competition law that leverages interoperability and open standards, in additional to traditional legal methods.

We look forward to continuing to engage with you and other stakeholders in the Government of India on formulating India's national e-commerce policy. If you have any questions about our submission or if we can provide any additional information that would be helpful as you continue your important work, please do not hesitate to contact Mozilla's Policy Advisor Amba Kak at amba@mozilla.com.

I. Data as a "national asset"

The Policy posits the data of Indians as a *"collective resource, a national asset, that the government holds in trust, but rights to which can be permitted"*. We object to this framing at multiple levels as it paves the way for policy proposals that undermine individual rights and is in stark contrast to the expectations of Indian internet users. Moreover, this policy conflates the government's interests with society's interests, which is a dangerous assumption for the world's largest democracy.

This framing, founded on a flawed model of data ownership, undermines the Supreme Court of India's decision in *Puttaswamy v Union of India* as well as India's commitments under the International Covenant on Civil and Political Rights. The *Puttaswamy* judgment held in no uncertain terms that the fundamental right to privacy was "an intrinsic part of the right to life and liberty", predicated on the dignity and autonomy of every individual. To replace this fundamental right with a notion of ownership akin to property, vested in the individual but easily divested by state and non-state actors leaves individual autonomy in a precarious position.

The goal of data-driven innovation oriented towards societal benefit is a valuable one. However, any community-oriented data models must be predicated on a legal framework that secures the individual's rights to her data, as affirmed by the Constitution. Without these protections, there is nothing to prevent the government or any business (foreign or domestic) from exploiting data in ways that contravene the autonomy and dignity of the individual in question.

The Policy also notes the value of "anonymized and aggregated data" towards creating these "data commons". As we argue in subsequent sections, we acknowledge and support the release of more open datasets that might spur innovation in India. However, we would also warn that research has consistently shown that there are serious risks of reidentification even with apparently anonymized datasets. Paul Ohm's seminal paper concluded that

"Data can be either useful or perfectly anonymous but never both." A study by Latanya Sweeney found that 87.1% of people in the United States were uniquely identified by their combined five-digit ZIP code, birthdate, and sex. Another study re-identified data subjects based purely on their movie preferences on Netflix. In light of these risks, we would urge the government not to make the blanket assumption that the public release of datasets is an acceptable risk.

II. Restrictions on storage, sharing, and cross-border flow of data

The Policy proposes a series of broadly worded strategies targeted at the data of Indians' held outside of India. These range from requirements for local storage of data on servers in India, to multiple restrictions on sharing of data with foreign companies and governments, to requirements to provide adequate notice for data collection. By way of contrast, the Policy posits that the Government of India should have broad access to the data of Indians, requiring that any entity that stores data abroad must "comply immediately" with any request for data from "Indian authorities."

It is unclear what objective the Policy seeks to achieve with this medley of strategies. At certain points, the policy notes that these restrictions might ensure greater privacy and security for the data of Indians. This objective, however, would be better served by a strong data protection law accompanied by meaningful surveillance reform. The MEITY Draft Personal Data Protection Bill makes a strong start. With certain key amendments, such as strengthening the regulation of data processing by government and surveillance agencies' and bolstering the independence of the data protection authority, we believe that the passage of the data protection law could be a major step forward towards protecting the privacy of Indians.

Without these reforms, localizing data in servers in India is more likely to make personal data more susceptible to overbroad access by law enforcement and surveillance agencies. As the Justice Srikrishna Committee has noted, surveillance reform in India is much overdue and currently there are little to no procedural safeguards around government surveillance. While surveillance may be a legitimate function of the state, these are powerful tools in the hands of government agents and should be subject to accountability, transparency, due process, and meaningful limits. This follows from the Supreme Court's diktat in *Puttaswamy v. Union of India* where a unanimous verdict held that any state interference with privacy must be subject to tests of legality and strict proportionality. Given that the current

legal framework falls short of these standards, a broad localisation mandate is likely to mean even fewer checks on the power of the government to access personal data.

Moreover, storing a copy of all personal data pertaining to Indians in a handful of locations could create a "honey pot" for malicious actors, thereby increasing the risk of a breach with a profound effect on India's citizenry. In comparison, distributing storage of data across a network of servers globally means that there is no concentrated point of attack or single point of failure. Many businesses might find that this mandate would jeopardize the security of the personal data they have been entrusted with, with implications for users globally, not just in India. Finally, while large companies could more easily afford the additional costs associated with this data localization mandate, the expense of compliance may prove disproportionately harmful to small businesses and start-ups.

There is also a meaningful distinction to be made between mandatory data localization regimes -- which require data to be stored within the borders of a given country unconditionally -- and some of the limitations on data transfer found in data protection laws, including the GDPR and MEITY's Personal Data Protection Bill. These laws provide for a variety of options, including standard contractual clauses, binding corporate rules, and determination of adequacy for countries or sectors. While we believe it would be in India's interest to avoid any restrictions on the cross-border transfer of data, we recognize the government's legitimate interests in ensuring the protection of Indians' privacy.

III. Disclosure of source code

The Policy also endorses the disclosure of source code from foreign companies on the grounds that this would facilitate *" transfer of technology and development of applications for local needs, as well as for security"*. As an open source organization, we make our code publicly available, but we recognize that companies do have legitimate interests in protecting their source code for security and commercial considerations.

Allowing the government discretion to require access to source code presents a number of risks to the reputation of Indian and foreign businesses alike. Notably, the Policy does not state which entities the government anticipates forcing companies to share source code with. The sharing of source code with the government could not only facilitate unauthorized government

surveillance, but it's unlikely that the government could guarantee that this information would be secure from malicious third-party actors. This would present real privacy and security risks to Indian users. Moreover, if the source code of some of the largest companies were to be stored in a centralized database, there is a serious risk that this sensitive information would be compromised by some of the most powerful foreign adversaries in the world. This requirement will only undermine trust and confidence in the products/services that companies provide, and would create a significant barrier to doing business in India.

IV. Access to data and competition

The Policy aims to counter the *"high barriers to entry created by larger market entities in the digital sector"* through requirements that these large market entities share data with smaller firms entering the market. Data driven innovation can unlock great benefits to individuals, businesses, and society. In this spirit, Mozilla, recently released "Common Voice", the largest open dataset of human voices available for use by start-ups, researchers, and the general public.

The focus on increasing the competitiveness of the digital economy is both necessary and timely, given the global concentration of market power in a handful of firms. In some cases, the Government could promote competition in the digital economy by supporting dominant firms to grant potential competitors access to privately held data. However, we would urge the government to approach this strategically and encourage this data sharing through a targeted incentive-driven framework, rather than imposing blanket coercive measures that will alienate global companies and likely raise legal challenges. We would also urge the government to make this one prong of a broader reform of competition law.

- Any approach to enable data sharing will have to ensure that robust privacy safeguards are in place. A data protection law must be in place which would ensure that all personal data is excluded from any data sharing. As noted earlier, any such policies would need to mitigate the risks of inadvertent reidentification of individuals through combining apparently anonymized data points.
- Rather than blanket coercive measures to open up datasets, the government should conduct an exercise to identify those aggregate and anonymised datasets that would be most valuable to new, nascent businesses. As noted in the UK Governments' recent Digital

Competition Expert Panel Report, there are already a number of positive examples of such voluntary data sharing. For instance, Uber has chosen to release anonymised and aggregated data under the 'Uber Movement' scheme to inform and improve infrastructure and planning decisions.

- There are other technical measures beyond data sharing which could facilitate greater competition in additional to traditional legal methods. Specifically, competition policy should encourage designing for interoperability and standards-centric design and implementation, coupling positive incentive "carrots", including potential safe harbours, with corresponding "sticks" of heightened merger review standards and strengthened enforcement of rules and policies against anti-competitive behaviour by firms.

Conclusion

As the creator of an open source and privacy-focussed browser, we support the consideration of measures aimed at increasing the competitiveness of the digital economy, offering more meaningful choices of Indian users, and ensuring that their privacy is protected. However, for the reasons outlined above, we believe the current draft of the Policy is not fit for purpose. We hope the Department will consider our recommendations and continue to conduct wide and broad-based consultations on these important issues.