675 Third Avenue, 3rd Floor
New York, NY 10017-5704, USA
t: +1-212-642-1700 | f: +1-212-768-7796
inta.org | info@inta.org

March 16, 2022

Ms. Kavita Bhatia
Scientist F
Ministry of Electronics and Information Technology
Government of India

Email: kbhatia@gov.in; pmu.etech@meity.gov.in

Dear Ms. Bhatia:

Re: Data Privacy Principles and Considerations for India (Comments to the Draft India Data Accessibility & Use Policy 2022

The International Trademark Association (INTA) is a global association of brand owners and professionals dedicated to supporting trademarks and related intellectual property (IP) to foster consumer trust, economic growth, and innovation. In line with our mission, INTA has been monitoring legislative trends and global initiatives regarding privacy laws that have been in a state of flux in recent years.

With these principles in mind, INTA takes this opportunity to provide its perspective on issues which are of importance to brand owners when it comes to privacy and data protection laws. We thank the Government of India for providing this opportunity to comment on The Draft India Data Accessibility and Use Policy 2022 (the Policy). Our comments are organised by general themes as applied to the Policy and related privacy considerations. INTA is pleased to share its experience and welcomes the opportunity to engage in discussions on the topic.

I. Privacy Trends and India

Although legislation varies considerably by jurisdiction, global data privacy legal norms generally support the principles of data processing, namely, lawfulness; fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; disclosure for legitimate purposes; and accountability.

INTA notes the current trends in data privacy regulation globally and in India. India has over 700 million internet users and over 400 million smart phone users. India generates 150

exabytes of data annually.[1] The digitizing trends and implementation across industries has been addressed with the Government of India taking significant steps in tech policy and data regulations including in respect of personal data, non-personal data, health data, financial data, and data related to e-commerce and other consumer-facing services. Particular mention is made of the Information Technology Act, 2002 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, dealing primarily with protection of data in electronic form.

INTA further notes that several pieces of legislation and policy are currently underway and being debated in India, including the Personal Data Protection Bill 2019 (PDP Bill), which was tabled in Parliament by the Ministry of Electronics and Information Technology (MeitY) in December 2019. A joint parliamentary committee (JPC) was set up in 2019 to review the PDP Bill. The report of the JPC was presented and tabled before both Houses of the Indian Parliament on 16th December 2021. INTA understands from press reports in India that the PDP Bill may be refreshed to cover the technology landscape in a more comprehensive manner.[3] In the event that the PDP Bill is updated, INTA would ask that the considerations highlighted in this letter that relate to data privacy are incorporated in the instances where they may not have been incorporated in the current version.

In its current form, the PDP Bill seeks to implement measures that will bring significant transformation to the data protection landscape in India. The PDP Bill stipulates compliance requirements for all forms of personal data. It broadens individuals' rights, introduces a central data protection regulator, and stipulates data localization requirements for certain forms of sensitive data. The PDP Bill applies extra territorially to non-Indian organizations where nexus requirements are met. Significant financial penalties for non-compliance are also prescribed. It is noted that key issues under the PDP Bill which continue to be debated include data localization and the Government's access to data.

In addition to the protection, the legislative and policy framework seeks to effectively manage and use datasets for economic growth, recognizing data as a valuable intangible asset. The report of the JPC understandably notes concerns of sharing and using personal data by third parties without the consent of the concerned individuals. Concern is also noted in the report about violations of sovereign laws.

To address concerns on data access, the Ministry of Electronics and Information Technology (MeitY) has invited comments to the Policy. The Policy addresses access by private stakeholders of non-personal data held by Government. It proposes a regulatory authority called

[1] Report dated December 2021 of the Joint Parliamentary Committee to the PDA Bill. https://www.ahlawatassociates.com/wp-content/uploads/2021/12/17-Joint-Committee-on-the-Personal-Data-Protection-Bill-2019.pdf

[3] See https://economictimes.indiatimes.com/tech/technology/fresh-legislation-may-replace-data-protection-bill/articleshow/89624369.cms

the Indian Data Council (IDC) and an agency called India Data Office (IDO) to oversee framing metadata standards and enforcement.

The legislative and policy measures in the Policy, addressing access by private stakeholders of non-personal data held by Government, proposing a regulatory authority called the Indian Data Council (IDC) and an India Data Office (IDO) to oversee framing metadata standards and enforcement, are notable advancements in protecting data, both personal data as well as non-personal data. Promoting the core principles and global best practices in data management including collection, disclosure, access and use, INTA believes these principles go a long way in boosting confidence among stakeholders in the growing economies. With growth in technology and innovation, stakeholders own valuable IP assets which are either held or used in India and which greatly contribute to the growth of the Indian economy. Imperative within the proposed legislative and policy framework is, therefore, access of data by IP owners for the protection and enforcement of their valuable IP within India.

Identification of potential offender individuals is critical for timely protection and enforcement of IP. Access to accurate data in such circumstances is essential. Often, pertinent data for such actions include the personal data of both natural and juristic persons, particularly where such data has been used for commercial or malicious purposes.

INTA recognizes the rights of privacy of all individuals and their right to keep their personal data from disclosure. INTA is also confident and hopeful that the Policy will incorporate a mechanism with special criterion for data access to IP owners for information as may be required for the protection and enforcement of IP assets. To this end, INTA's recommendation includes striking a balance between the rights of individuals and the rights of IP owners.

II. Certainty in Enforcement Mechanisms and Obligations

Following our analysis of these laws, we have highlighted several nuanced issues of importance to brand owners. For example:

1. To provide certainty on enforcement mechanisms for noncompliance with the Policy and what scope of fines and penalties can be issued by the government; and
2. To provide guidelines that are issued by the regulatory bodies and can be used by brand owners to help ensure they are compliant with the Policy. Therefore, there is now an opportunity in the Policy to clarify the obligations of brand owners and we have identified ways to achieve this goal going forward.

III. Privacy Laws Should Not Be Unduly Onerous

When considered in connection with the Policy, data privacy laws should seek a balance between protecting the interests of data subjects and the interests of businesses engaging in international trade. Therefore, any proposed regulations should consider the amount of personal data processed and the size (by revenues) of the processor. Requirements to consider are:

1. Annual gross revenues.
2. Whether the processing entity, alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of a defined number of consumers, households, or devices; or
3. Whether the processing entity receives a defined percentage or more of annual revenue from sales of consumers' personal information.

The necessary balancing focuses the rights of the data subject to limit access to and use of his/her data against the rights of a business to access and use the data for a legitimate purpose, whether that is to provide goods and services or to protect the intellectual property rights of the business, or to comply with general regulatory requirements.

IV. Timelines for Legal Compliance Should be Reasonable

Another key concern for brand owners (especially internationally known brands) is the importance of ensuring there is ample time allotted to ensure timely compliance with data protection regulatory requirements. Large international brands are known to have robust internal governance policies. While these policies are created to foster accountability and due process, it can take time to update and modify policies to adhere to new government requirements. Providing reasonable timeframes for compliance with new data privacy laws will let brand owners analyze the statutes and create procedures to comply with the new requirements and implement them. Lastly, a process for seeking an extension of time for compliance should be simple, cost-effective, and freely given when presented with evidence of good faith attempts to comply with the new laws.

V. Data Privacy Laws Should Facilitate Access for Legitimate Trademark Enforcement Purposes

Addressing the issues raised above creates a business-friendly environment for brand owners (local and foreign) without compromising on sound consumer data privacy principles. One of the principles envisaged under the Draft on which data sharing and governance needs to be based is protection of Intellectual Property as noted in Clause 5.12 of the Policy. Therefore, the legitimate rights of trademark owners should be considered when developing and weighing policies on access to personal information. Some laws have the unintended consequences of restricting access to data necessary for the purposes of trademark enforcement. To protect consumers, any new data protection laws should not interfere with brand owners' ability to access records important to trademark enforcement and counterfeit investigation.

1. An example of a current law inhibiting enforcement is the European Union's General Data Protection Regulation (GDPR). While GDPR was written with the intent of creating a balancing test for some levels of data disclosure, there have been unintended consequences in the matter of providing access to information

for law enforcement, intellectual property protection and cybersecurity research. Interpretations of GDPR by the Internet Corporation for Assigned Names and Numbers (ICANN) and the European Data Protection Board concluded that the formerly public-facing data that was available related to the ownership of a domain name (known as "WHOIS data") could no longer be published. GDPR, and the accompanying European Law Enforcement Directive, lacks any specific provision to allow for brand owners and even law enforcement to access information for the purpose of exercising rights of enforcement or anti-counterfeiting or anti-abuse measures, or explicitly shield data controllers from liability for disclosing data for such legitimate purposes.

2. New privacy legislation should assist in lowering the obstacles to protecting the public from trademark infringement or counterfeit products by expressly allowing for an expeditious procedure to provide access to brand owners and law enforcement to records related to domain name ownership or other non-public information. Access should be granted provided such request can be shown to be reasonably related to a legitimate investigation (which may or may not include a Court order), while at the same time requiring that data processing principles be upheld with respect to the use of such information.

3. Data that does not belong to a natural person is not personally identifiable data. Data that identifies juristic persons —such as entities that offer goods or services online to the public—through registered domain names in databases like the WHOIS domain name database, is not personally identifiable data and should be freely processed and published to protect consumers and assist rights holders and law enforcement agencies in legitimate commercial investigations. This approach, while sharing or governing non-personal data, aligns with the principles of intellectual property protection.

4. Data that is patently false or fictitious is also not personally identifiable data, and it should also be freely processed and published to protect consumers and assist rights holders and law enforcement agencies in legitimate investigatory and enforcement actions. There is an opportunity for new legislation to instill verification and validation principles whereby data is both subjectively accurate to the data subject and objectively accurate to the rest of the world. This approach, while sharing or governing non personal data, aligns with the principles of intellectual property protection.

There is an opportunity for new legislation to clarify the obligations of brand owners and to ensure continuous robust trademark enforcement to avoid brand confusion and counterfeiting, while at the same time protecting consumer privacy. This would avoid the unintended consequences that we have seen with certain other data protection legislations and regulations in other jurisdictions.

VI. Applicability of these considerations to the Draft India Data Accessibility and Use Policy

Based on the foregoing and in addition to Clause 5.12 referenced above, INTA has analyzed the Policy and highlights the following additional points for consideration:

1. The Policy intends to "*harness public sector data for catalysing large scale social transformation.*" All non-personal data in possession of the government will be available for licensing and sharing under this Policy unless it has been categorised as non-shareable. Based on this intention, INTA supports the proposition that the powers to prepare and implement such a Policy should flow from a legislation that governs data protection. The introduction of the Policy, in the absence of a legislation governing data protection, would mean that individuals/citizens are left without any remedy in case of misuse of data and thereby, the violation of the right to privacy.

2. Currently, no legislation sets any limitations on the kind of data that may be collected, or which specifies that certain kinds of data cannot be converted into non-personal datasets. The aforesaid issues concerning non-personal data should be legislated upon before a Policy governing its licensing is passed.

3. Clause 4.1 of the Policy specifies that the policy is not only applicable to "*all non-personal data*", but also to "*information created/generated/collected/archived by the Government of India directly or through authorized agencies by various Ministries/Departments/Organizations/Agencies and Autonomous bodies*". It is evident from a plain reading of clause 4.1 that even personal data has been brought within the ambit of the Policy, while the type of data that has been referred to throughout the rest of the Policy is only non-personal data. It is therefore arguable that the Policy potentially allows the sharing of health data collected under the Arogya Setu Covid tracking application, as well as other data collected for issuance of Aadhar national identification numbers and, PAN tax account numbers, etc. This uncertainty may create unintended consequences for the licensing and the processing of the data for business purposes.

4. Clause 4.2 of the Policy allows the state governments to adopt the provisions of the Policy, "as applicable". This grants immense discretion to the state governments in terms of setting any limitations on its powers, while placing no restrictions in terms of sharing or acquiring non personal data. This can promote uncertainty in terms of various state responses and create confusion for those who wish to comply with the law.

5. Clause 6.6 of the Policy allows "*stakeholders including researchers, start-ups, enterprises, individuals and government departments*" to access non personal data and evidently, by virtue of this clause, all can access the non-personal data available with the government. While such data may be used to promote innovation, it is imperative to have clear guidelines as to what is acceptable and unacceptable including ethical guidelines to inform those uses.

Addressing the foregoing considerations is imperative to facilitate necessary means of trademark enforcement and brand owner compliance when drafting new data governance and privacy laws and regulations, thereby achieving the goal of providing robust consumer protection. We hope that our views are considered and are encouraged as focal deliberation topics as India deliberates its new Policy.

For further information on INTA and its policy positions, please contact Lori S. Schulman, Senior Director, Internet Policy, INTA (lschulman@inta.org) and Gauri Kumar, India and South Asia Consultant, INTA (gkumar.consultant@inta.org).

Thank you in advance for considering the views of INTA.

Yours sincerely,

Gauri Kumar
India and South Asia Consultant
International Trademark Association

About INTA

The International Trademark Association (INTA) is a global association of brand owners and professionals dedicated to supporting trademarks and related intellectual property (IP) to foster consumer trust, economic growth, and innovation. Members include nearly 6,500 organizations, representing more than 34,350 individuals (trademark owners, professionals, and academics) from 185 countries, who benefit from the Association's global trademark resources, policy development, education and training, and international network. Founded in 1878, INTA is headquartered in New York City, with offices in Brussels, Santiago, Shanghai, Singapore, and Washington, D.C., and a representative in New Delhi. For more information, visit inta.org.