ECONOMIC LAWS PRACTICE
ADVOCATES & SOLICITORS

DATA PRIVACY & PROTECTION IN INDIA: AN UPDATE

FOREWORD

Dear Reader,

We welcome you to the latest edition of ELPs update on 'Data Privacy & Protection in India'.

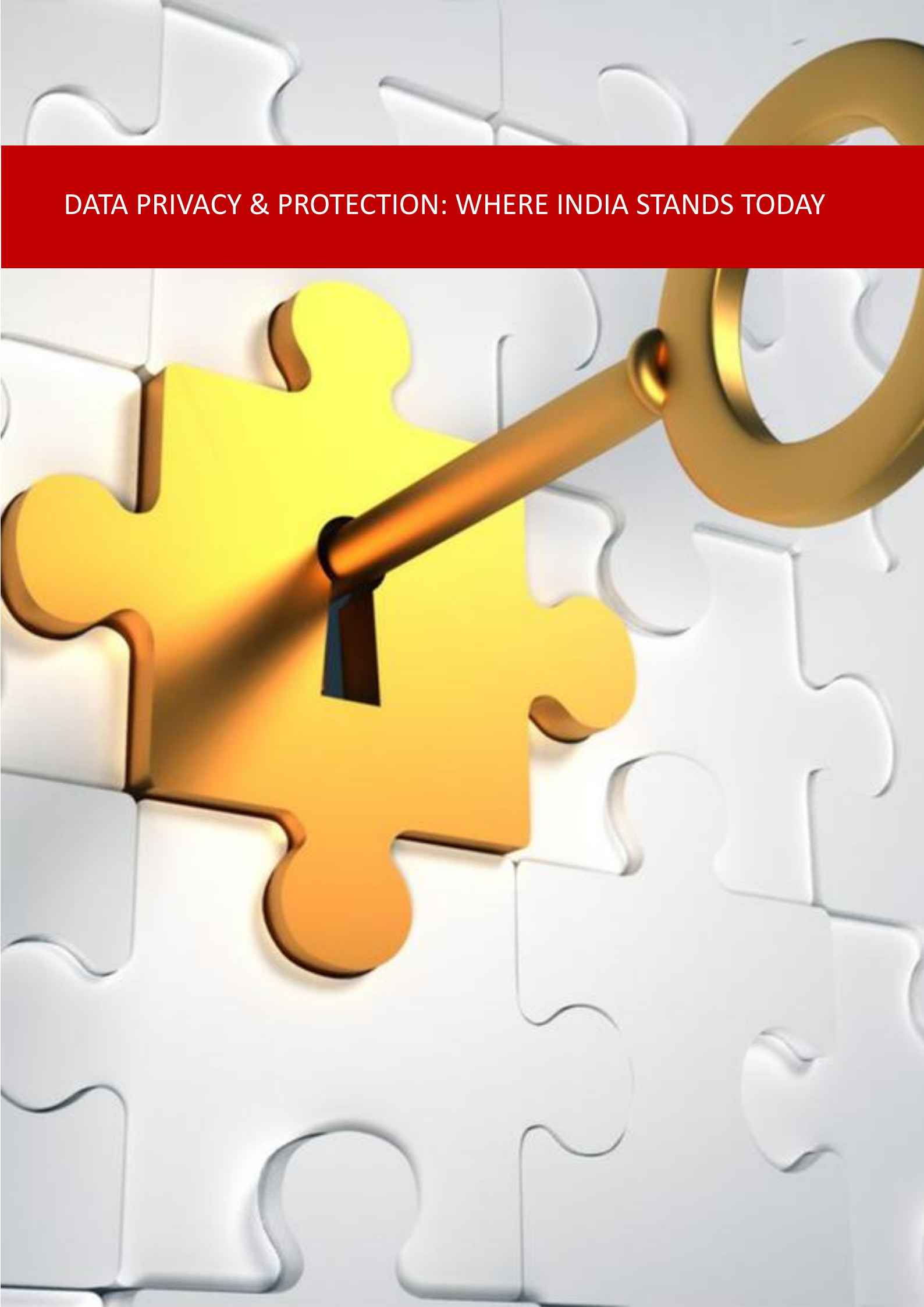
In this document, we examine, through various articles, India's data privacy and protection norms, an analysis of the proposed Personal Data Protection Bill, potential competition law risks faced by technology businesses in India and cost ramifications arising from domestic and bilateral or international data privacy compliance requirements.

We hope you will find this information helpful. For any clarification or further information, please connect with your point of contact at ELP or reach out to us at insights@elp-in.com.

Regards,

Team ELP

DATA PRIVACY & PROTECTION: WHERE INDIA STANDS TODAY



Change is inevitable. Every new phase though brings with it a two sided coin of opportunity and complexity. So also, the phenomenal rise of India's digital economy, has created a new challenge of inherent tension between the growth of India's digital economy business and the protection of personal data. Even more intriguing is that the full potential of the data is not known. As technology progresses, newer applications emerge enhancing the value of the data.

Several questions beg consideration though: who does this data belong to? Who can access it? What are the limits, if any, on the exploitation of this data? As in all things in technology, the law is playing catch up. Jurists around the world are struggling to marry traditional concepts of the law and the absurdly invasive times we find ourselves in. This position is further complicated by several governments demanding and seeking access to data from its citizens and corporates. On the other hand, what are the limits to privacy? Can data be demanded for the availing of basic services, travel or even government benefits? Does national security override all concerns of privacy?

On August 24, 2017, the Supreme Court of India provided clarity on a number of these issues. The judgement [1] held that the 'right to privacy' is a fundamental right guaranteed by Part III of the Constitution of India. This decision has and will continue to have far-reaching ramifications on the laws and regulations. New laws will now be tested on the same parameters on which the laws that infringe upon person liberty are tested under Article 21 of the Constitution of India. The right to privacy is now unequivocally available – the question that still remains outstanding is its contours and limits.

As on date, India does not yet have a comprehensive legislation which deals with data protection and privacy. The existing legislations and policies are essentially sectoral in nature. Apart from other sectoral legislations, as of now, the relevant provisions of Information Technology Act, 2000 and the rules thereunder, regulate the collection, processing and use of 'personal information', and 'sensitive personal data or information' by a 'body corporate' in India.

With the intent to formulate a comprehensive data protection legislature, the expert committee set-up under the chairmanship of Justice Srikrishna for formulation of data protection regime in India has, after a year of deliberation, released the Personal Data Protection Bill, 2018 ("**Proposed Bill**") along with a report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" in the public domain. This report is considered to be a key landmark towards India's move in the direction of increasing data security norms.

The article below aims to capture the key concepts and the potential concerns surrounding the Proposed Bill.

Key Concepts- Personal Data Protection Bill, 2018

The Proposed Bill aims at regulating the processing of personal data as a recognition of an individual's right to privacy. While still not a law, the Proposed Bill provides a glimpse into what the data protection regime in India may look like, including the rights and obligations of the participants.

The Proposed Bill seeks to adopt a fourth path, distinct from (a) US's *laissez-faire* policy where consent of the data owner is the basis for usage of data (b) EU's comprehensive legal framework delineating rights and obligations of users and processors, and (c) China's data protection framework focussing on addressing national security risks.[2]

Nature of Personal Data Aimed to be Protected

"Personal data" is a unique identification methodology which is based not only on body attributes but any data relating to a natural person who is directly or indirectly identifiable, having regard to any characteristics, trait, attribute or any other feature of the identity or any combination of such features with any other information of such natural person.

Territorial Application

The Proposed Bill has a wide applicability and is not restricted in its application to data collected, disclosed, shared or processed within India, or data processed by Indian citizens or organisations but also extends to data fiduciaries/data processors not present in India, which engage in the activity of processing of personal data in connection with business carried out in India or a systematic activity of offering goods and services to data principals in India or activity which involves profiling of data principals in India, thus having an extraterritorial jurisdiction.
The Proposed Bill would, however, not apply to anonymised data which has been transformed by an irreversible process so that the data principal cannot be identified.

[1] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors [2017 (10) SCALE 1]

[2] *New China Data Privacy Standard Looks More Far-Reaching than GDPR,* Centre for Strategic and International Studies. Available at: https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr

Basis for Processing Personal Data

(i) On the basis of consent:
   a. given prior to the commencement of processing;
   b. which is free, informed, specific, given through affirmative action (not implied), and being capable of withdrawal with the same ease with which it was granted;
   c. where provision of goods or services, their quality, enjoyment of legal rights etc. are not conditional upon such consent being provided if not necessary for that purpose;

(ii) If necessary for the function of the State;

(iii) If explicitly mandated by Indian law or required for compliance of an order of the court or tribunal in India;

(iv) If necessary for prompt action in case of medical emergency or during epidemic or disaster or public disorder;

(v) For the purpose of employment; and

(vi) For reasonable purposes as notified by the data protection authority.

Cross-Border Transfer of Personal Data

(i) Data Mirroring: data fiduciary to store, on a local server in India, at least one serving copy of personal data processed;

(ii) Data Localisation: Critical personal data to be stored **only** in India;

(iii) Permitted Transfers: personal data can be transferred outside India:
   a. on the basis of standard contractual clauses or intra-group schemes that have been approved by the data protection authority;
   b. to notified countries approved by the data protection authority; or
   c. with approval by the data protection authority for a particular transfer or set of transfers as permissible due to a situation of necessity.

Key Concerns

- **Anonymisation of Personal Data:** The Proposed Bill exempts from its ambit the processing of anonymised data. But for personal data to be considered as anonymised data, it needs to undergo irreversible process of transformation or conversion to a form in which data principal cannot be identified. However, as the technology evolves, certain anonymised data could become capable of de-anonymisation, therefore, determining whether the process is irreversible or not may not be possible.

- **Data Mirroring:** The data mirroring requirement has been included to enable effective enforcement of local laws. However, this requirement may lead to excessive burden being cast upon organisations having global presence to retain a copy in India as some of these organisations may prefer storing all personal data on central cloud servers at cheaper costs, instead of storing data locally in each jurisdiction.

- **Data Breach:** Not all data breaches are required to be notified by the data fiduciary to the data protection authority, only those breaches which are likely to cause harm to any data principal are required to be notified. Therefore, it is up to the data protection authority to determine whether such breaches are likely to cause harm to data principals and consequently should such breach be notified to the affected data principals. This could reduce the amount of control that a data principal can exercise over his/her personal data.

- **Bar on Cross-Border Transfer of Critical Personal Data:** In today's globalised world cross-border flow of personal data has become a norm instead of an exception, the data localisation requirement hinders such free flow of data. It also raises concerns surrounding India's obligations under the World Trade Organisation. The argument in the favour of this requirement is that it will minimise the vulnerability of relying solely on undersea cables for transmission, help in harnessing data for growth of Artificial Intelligence, and prevent foreign surveillance risks. At this stage it is unclear as to the nature of personal data sought to be included in this category. But this could nevertheless have economic as well as market implications.

- **Excessive Delegation of Power**: The data protection authority has been granted wide powers under the Proposed Bill to make regulations consistent with the main enactment including notify further categories of sensitive personal data, categories of personal data requiring additional safeguards, factors to determine appropriateness of age verification, circumstances where data protection impact assessment shall be mandatory, classifying certain data fiduciaries as significant data fiduciaries which are subject to additional compliance requirements etc. These extensive powers can be exercised by the data protection authority without necessarily being subjected to Parliamentary debates.

- **Processing of Data for Reasonable Purposes:** It is unclear at this stage as to what is sought to be covered as a ground for processing personal data for '*reasonable purposes*'. The factors that will be considered while determining reasonable purposes are prevention and detection of unlawful activity, whistle blowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, and publicly available data. Given the substantial scope of these factors, in reality, the processing of personal data for reasonable purposes could end up diluting the rights granted to the data principal under the Proposed Bill.
- **Right to be Forgotten not Absolute:** Under EU-General Data Protection Regulation ("**GDPR**"), the data subjects have the right to obtain from the controller the erasure of his/her personal data without undue delay. On the other hand, under the Proposed Bill, the data principals can only restrict or prevent continuing disclosure of personal data by the data fiduciary and not seek complete erasure. Also, such right can be exercised only with the approval of the adjudicating authority. Making the right to be forgotten substantially limited and not absolute.
- **Exemption for Compliance Requirements:** Extensive exemptions from compliance with the provisions of the Proposed Bill have been granted for processing of personal data not only on account of security of the State, and prevention, detection, investigation, and prosecution of offences, but also for journalistic purposes. This could possibly lead to undue intrusion in private citizens' lives without having the protection of right to privacy granted as a fundamental right under the Constitution of India.
- **Certain Offences Cognizable and Non-Bailable:** In addition to stringent penalties which may extend upto Rs. 15 crore or 4% of the total worldwide turnover of the preceding financial year, the Proposed Bill also makes certain contraventions cognizable and non-bailable offenses, punishable with imprisonment which may extend upto 5 years. Given that stringent financial penalties could act as sufficient deterrent, introduction of criminal offences may not have been necessary. Further, making such offences cognizable and non-bailable could lead to misuse of such provisions.
- **Privacy by Design**: The concept of privacy by design which is present in GDPR has also been included in the Proposed Bill. The Proposed Bill requires data fiduciaries to implement policies and procedures to ensure '*legitimate interests of businesses including any innovation is achieved without compromising privacy interests*'. However, it is not clear as to what exact measures are the data fiduciaries required to undertake to achieve these objectives and further light needs to be shed to have greater clarity.
- **Setting-up of the Separate Appellate Tribunal:** As per the Proposed Bill, imposing of penalties and awarding compensation will be done by the Adjudicating Officer. An appeal against the order of the Adjudicating Officer can be filed with the Appellate Tribunal. Setting-up of the Appellate Tribunal and appointing of the Chairperson and the members of the Appellate Tribunal could, in all practicality, push the timelines for rolling out the Proposed Bill.

Conclusion: What Happens Next?

The Proposed Bill has generated huge interest and debate among various stakeholders including businesses, academia, citizen interest groups and think tanks. On one hand, the proponents of privacy rights are pushing for stringent data protection measures while on the other, the businesses argue that the increased costs of data protection compliance may make businesses unviable. One of the main criticisms of the Proposed Bill has been that it seeks to protect data as an end in itself, rather than means to an end. Undoubtedly, the Bill is likely to undergo significant churning through debates and reviews and it remains to be seen how India draws a balance between these two competing interests.

As Justice Srikrishna himself has noted, *'The report is like buying new shoes. It's tight in the beginning but it will become comfortable over a period of time.'*

Glossary of Key terms

Processing: includes collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.
Data Fiduciary: A person/ entity which determines the purpose and means of processing data.
Data Principal: the natural person to whom the personal data relates.
Data Processor: A person or entity which processes data on behalf of data fiduciary.
Data Protection Authority: The authority established under the Proposed Bill to ensure compliance.

PRIVACY CONCERNS SURROUNDING AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016 ("AADHAAR ACT")

The Supreme Court of India by its decision in *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.* dated September 26, 2018 upheld the constitutional validity of the Aadhaar Act (except for Section 57 which permits private parties to use Aadhaar number for establishing identity of individuals). The primary argument against the constitutional validity of Aadhaar Act was that it infringes upon the right of privacy of individuals guaranteed under the Constitution of India.

Right to Privacy a Fundamental Right

Though right to privacy is a fundamental right, like any fundamental right, the right to privacy is not absolute and there can be reasonable restriction and instances when the State can infringe an individual's right to privacy. The Supreme Court had laid down the following three-fold test to evaluate when State can intervene with the individual's fundamental right: (i) the existence of law; (ii) a legitimate state aim; and (iii) proportionality – including balancing the right to privacy with other fundamental rights. A fourth limb was added by Justice Kaul in his separate (but concurring) judgment. According to Justice Kaul, there should be procedural safeguards within the interception framework to check against the abuse of state interference.

Aadhaar Act Meets the Test of Constitutional Validity

While testing the constitutional validity against the three-fold test discussed above, the majority judgement was of the view that:

- since the Aadhaar Act was passed through legitimate legislative process the first requirement is satisfied.
- with respect to the second requirement, the majority judgement held that since India is a welfare state, it is duty of the State to ensure that distribution of benefits of welfare schemes reach its intended recipients. Aadhaar has a very effective means of disbursement of welfare benefit to the poor and needy. As such, the State has a legitimate aim to implement the Aadhaar Act.
- finally, with respect to the third limb of the test, the majority judgment was of the view that in addition to right to privacy, an individual also has rights to food, shelter and employment. It can actually be argued that implementation of the Aadhaar Act would effectively strengthen these other rights. Hence there is a need to evaluate the cost of a breach to individuals' right through the Aadhaar Act against the benefit that would accrue to an individual as a result of implementation of Aadhaar Act.

Common Good v. Privacy

While considering the need for proportionality, the majority judgment also noted that there needs to be a balancing of two facets of dignity of the same individual whereas, on the one hand, right of personal autonomy is a part of dignity (and right to privacy), another part of dignity of the same individual is to lead a dignified life as well (which is again a facet of Article 21 of the Constitution of India). Therefore, in a scenario where the State is coming out with welfare schemes, which strive at giving dignified life in harmony with human dignity and in the process some aspect of autonomy is sacrificed, the balancing of the two becomes an important task. We, therefore, have to keep in mind humanistic concept of human dignity which is to be accorded to a particular segment of the society and, in fact, a large segment. Their human dignity is based on the socio-economic rights that are read in to the fundamental rights.

The Other View

The dissenting judgment by Justice Chandrachud was, on the other hand, critical of the Aadhaar Act. In view of the privacy safeguards, Justice Chandrachud was of the view that, adequate norms should be laid down for each step from the collection to retention of biometric data based on informed consent, which are lacking in the Aadhaar Act. He also stated that Aadhaar Act which disallows an individual access to the biometric information, which forms the core of his or her unique ID, violates the fundamental principle of ownership of an individual's data. Further, a leakage in the Aadhaar database would pose an additional risk to this data. In the absence of an independent regulatory and monitoring framework which provides robust safeguards for data protection, the Aadhaar Act cannot pass muster against a challenge on the ground of reasonableness under Article 14 of the Constitution of India. In conclusion, Justice Chandrachud's dissenting judgment stated that though there is a legitimate state aim, the existence of a legitimate aim is insufficient to

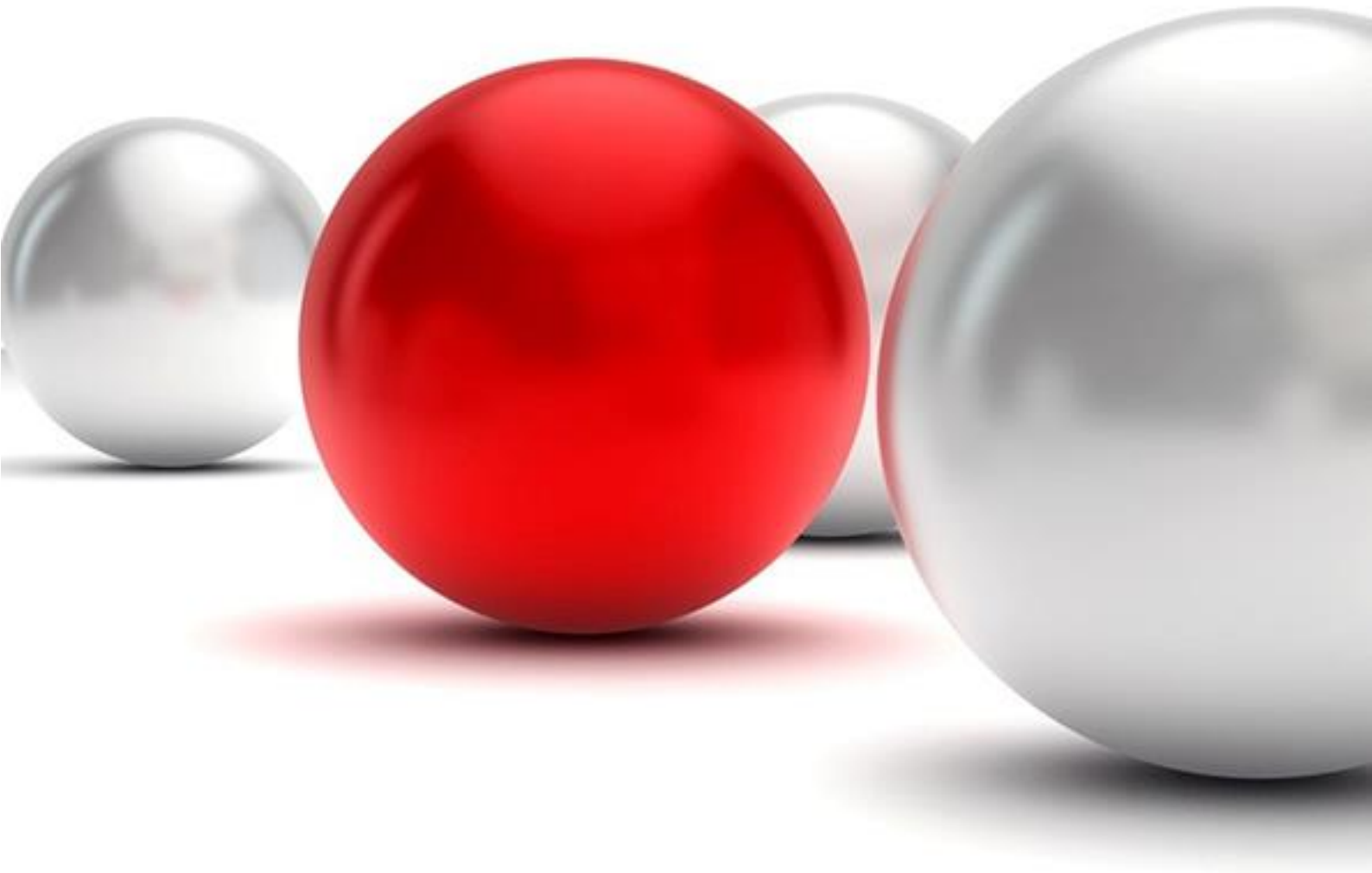
uphold the validity of the law, which must also meet the other parameters of proportionality spelt out in the right to privacy judgment.

Conclusion: Unanswered Questions

The Supreme Court's verdict has raised very pertinent questions for government and industry alike. Some doubts include: what would be the status of the Aadhaar numbers already collected? How would the registration of services without Aadhaar numbers now be done? What would be authentication mechanism in the absence of Aadhaar verification? Further, what implications would this have on ease of doing business and costs? How would delinking be of services from Aadhaar numbers be carried out? Would there be a penalty for companies which do not delink customer Aadhaar data?

No doubt, these apprehensions will be assuaged over time. However, the path to doing so will be a slow one.

DATA LOCALISATION: GENERAL OVERVIEW



Data localisation has become one of the most heavily debated topics in India in recent times. But India is not the first country to introduce such measures. Data localisation laws require that certain types of data be stored within the country's boundaries alone, although sometimes it is more broadly used to mean any restriction on cross-border transfer of data. Internationally, there has been an increase in data localisation legislation. Countries such as China, Russia, Indonesia, Vietnam already have data localisation norms in place. China localizes internet-based mapping services, critical information infrastructure and banking data. Canada localizes public interest data held by government agencies, schools and hospitals. Australia localizes health data.

The local storage of personal data has less to do with the privacy of individuals but more to do with ability of the enforcement agencies to enforce local laws, mainly data protection laws. Many countries introduce data localisation norms as local storage gives boost to law enforcement efforts by providing easier access to such information. However, such measures could lead to greater censorship of dissenting political voices, increased costs to global internet companies and limit access to global technologies such as cloud computing, internet of things, and big data analytics.

Analysing Data Localisation Laws from the lens of WTO

Additionally, the data localisation requirements and prohibition on cross-border flow of critical personal data may be argued to be inconsistent with India's obligations under the World Trade Organisation ("**WTO**").

Measures that regulate cross-border flows of personal data attract the provisions of the General Agreement on Trade in Services **("GATS")**, which governs international trade in services. Obstructions to the flow of personal data across borders may have direct implications on Mode 1 (cross-border services) and Mode 2 (consumption abroad). These restrictions and/or prohibitions in the cross-border flow of data: (i) *may* run afoul India's market access commitments, and (ii) *could* violate the national treatment requirements set out under the GATS since foreign service suppliers *may* be provided less favourable treatment compared to domestic service providers.

- **Market Access:** Article XVI of the GATS provides that, *inter alia*, where a country has made market access commitments in its GATS schedule, then that country is prohibited from imposing limitations, through any means, on the number of service suppliers, unless the country has included such limitation in its GATS schedule. Section 40 (1) and Section 40 (2) of the Proposed Bill could violate the market access commitments made by India in its GATS schedule. This is because these "measures" in the context of any supply of services provided in India could, in effect, limit the number of suppliers of that service in the Indian market. In other words, these provisions of the Proposed Bill could limit access of foreign firms to India's market by conditioning market access upon the local storage and processing of data. Such measures have the effect of restricting or prohibiting flow of cross-border services supply since they would require foreign firms to, *inter alia*, replicate data storage infrastructure which adds costs for additional data management and compliance requirements. However, this analysis has to be made on a case-wise basis after assessing the commitments made by India under the relevant service sector.

- **National Treatment:** The national treatment rule under the GATS applies to all sectors where specific commitments have been undertaken. These commitments prohibit WTO members such as India from discriminating in favour of their domestic companies. Specifically, Article XVII of the GATS makes an obligation on countries to accord services and service suppliers of other countries "treatment no less favourable than that it accords to its own like services and services suppliers." Article XVII:2 of the GATS specifies that a country may accord foreign services or service suppliers different treatment to achieve this objective. Article XVII:3 of the GATS defines treatment as "less favourable" if it "modifies the conditions of competition in favour of services or service suppliers of the Member."

  The national treatment obligation may come in the way of the data localisation requirements under the Proposed Bill. For instance, data localisation requires foreign suppliers to duplicate infrastructure and support-service in local markets. As a result, it could be argued that the foreign service suppliers are accorded less favourable treatment than the domestic service suppliers. Notably, even if the same conditions of localisation apply to national suppliers of *like* services or are "formally identical", it may be argued that they are still designed in a manner to alter the conditions in favour of *like* domestic service suppliers since they may not have to incur additional costs in replicating the infrastructure and support-service costs. Therefore, the possibility that such measures are viewed as "less favourable" under Article XVII of the GATS exists.

  Again, this analysis has to be made on a case-wise basis after assessing the commitments made by India under the relevant service sector. For example, data localisation requirements imposed by the Reserve Bank of India dated 6

April 2018 to Indian banks and authorized e-payment systems may not violate India's commitments at under the GATS. This is because India has made its commitments in financial services sectors subject to the requirements under its domestic laws through a horizontal exception. However, India has not provided for such a blanket exception in context of its commitments for other service sectors.

An Alternative Paradigm – More use of Bilateral and Multilateral Agreements

Discussions on how data localisation requirements could fall foul of the WTO norms have a strong support from most western economies. At this juncture, it would be worthwhile to evaluate an alternative approach to the issue surrounding free flow of data and data localisation.

The argument taken in the previous section was strongly based on the principle that personal data is like a "commodity" and hence could be traded. The catch-phrase 'data is the new oil' is a result of this idea. Extending this idea to the WTO, it is argued, that since data is like a commodity, it is essential that free flow of the data should be allowed under WTO norms. Hence, any effort to restrict this free flow of personal data through data localisation laws and without serious public policy reasons is a restraint on free trade.

The above suffers from numerous deficiencies in the Indian context.[3] At the threshold, it is important to evaluate if the WTO is at all an appropriate platform to take up issues surrounding transfer of data and consequently the question of data localisation. The following arguments could be made:

- First, norms on data privacy and ideas about the nature of personal data differ across the globe. While the US believes in a more market-based approach to the transfer of personal data; the EU, at the other side of the spectrum, caters to the rights-based approach that considers personal data an essential and extension of a person's identity and therefore more than a mere commodity. Coming to a consensus about the very nature of personal data itself at the WTO level could turn out to be problematic.
- Secondly, the use of WTO system could seriously undermine the democratic freedom and sovereignty of a nation which allows it to determine - by itself - what the most appropriate stance on an issue should be.
- Finally, various scholars[4] have argued that measures that are imposed to enhance civil liberties protections should not be tested through the lens of economic cost-benefit and efficiencies arguments.

It is our view that there exist varying levels of bargaining power, trade dependency and geo-political relationship of India with other nations. Instead of adopting a one-size-fit-all approach to data localisation, it would be desirable that India relies more on bi-lateral or multi-lateral agreements coving aspects of data transfer and transfer of personal data with similar mined nations.

It is to be noted that the EU also adopts this approach. Even though there exists a comprehensive data privacy law in the form of GDPR, the EU has a separate agreement with the US, called EU-US Privacy Shield, for a more customised approach to transfer of personal data especially to the US.

Existing Data Localisation Requirements

The argument surrounding data localisation is not new to India. Presently, there are certain sector specific requirements which require context specific data localisation:

- **Government Data:** Section 4 of the Public Records Act, 1993 prohibits the transfer of public records out of India without the approval of Central Government, unless such transfer is being made for an official purpose.
- **Payment Systems:** The Reserve Bank of India ("**RBI**") by its notification dated April 6, 2018 has mandated that all payment system providers shall ensure that the entire data relating to payment systems operated by them is stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. The last date of implementation was notified as October 15, 2018.

[3] For a more in-depth discussion on this please refer to: Hill R (2017). Second contribution to the June–September 2017. Open Consultation of the ITU CWG-Internet: Why should data flow freely?

[4] For example, Kuner, C. (2015). Data nationalism and its discontents. 64 Emory Law Journal Online 2089.

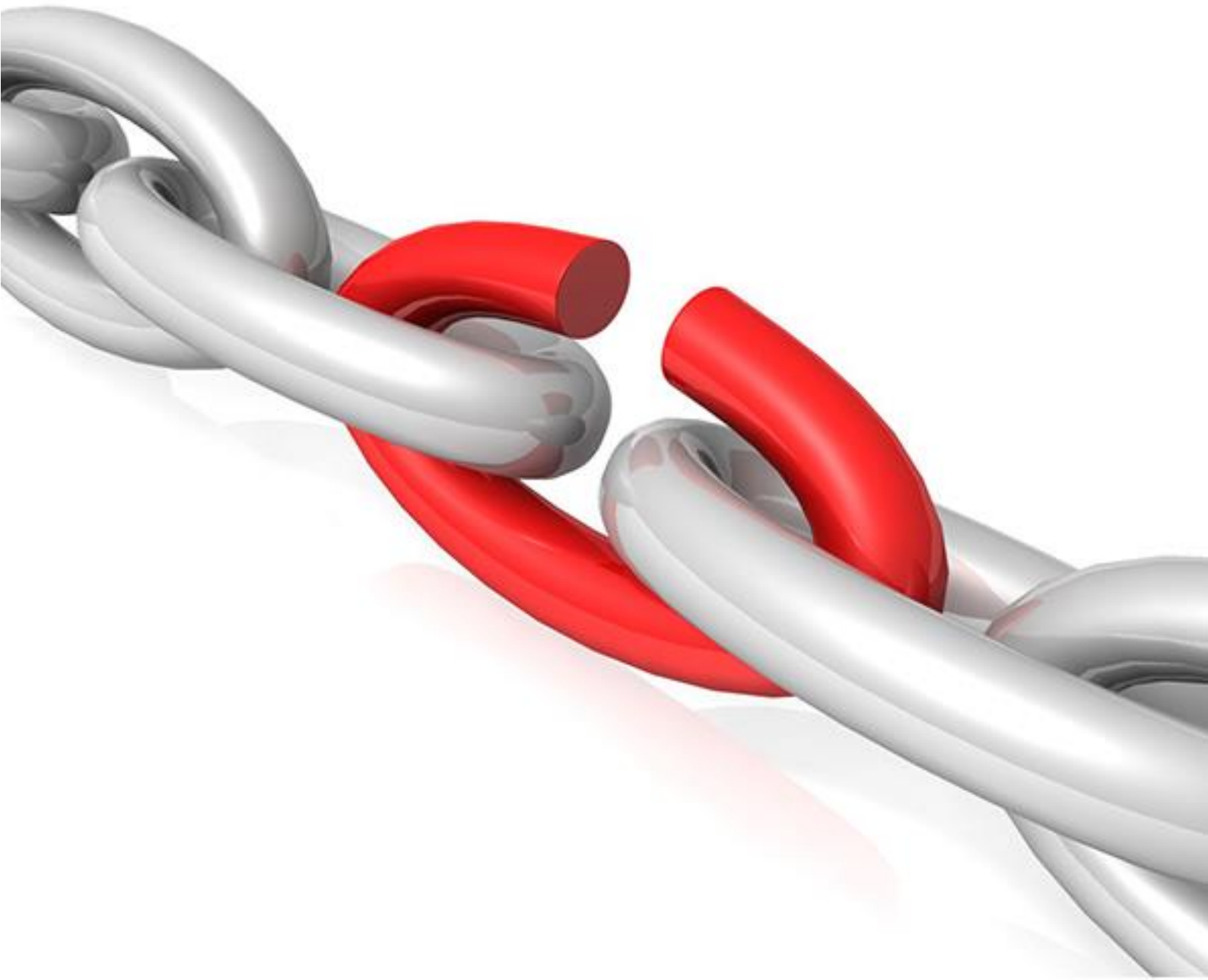
Conclusion: Big Uproar

There has not been much debate surrounding government data, but data localisation requirement by payment systems operators has seen a huge uproar. In light of the data localisation requirement, companies like Amazon, WhatsApp and Apple have put the plans of introducing their payment services in India on hold.[5] Despite the lobbying from industry bodies, RBI has not extended the deadline for compliance with the data localisation norms.

The main fear seems that other countries may follow suit and introduce similar measures. The other fear appears to be excessive government access and surveillance. The argument mostly made against the data localisation requirement is that local storage does not necessarily provide better access to data and leads to greater threat of data breaches. How this sensitive subject is dealt in India's comprehensive data privacy legislature still needs to be seen.

[5] https://www.fortuneindia.com/enterprise/rbi-data-localisation-rule-trips-apple-pay/102374

TECHNOLOGY & DATA-INTENSIVE BUSINESS: THE COMPETITION LAW VIEWPOINT



The global perspective

The last few years have seen many of the world's leading technology companies come under increasing scrutiny of competition regulators across the globe, with historic fines levied on them for a variety of business practices and other transgressions. The core concerns pertain to accumulation of large data sets by companies and their ability to process it through computer algorithms and artificial intelligence in a manner that may negatively impact competition, as well as the end consumer. Control over this large pool of data is increasingly becoming synonymous with 'market power', even as an increasing number of industries – ranging from agriculture to airlines – become reliant on 'big data'.

Technology and data-intensive business in cross-hairs of US and EU regulators: The regulation of technology and big data presents its unique challenges, evident from the divide even between the major global regulators. While the European Union has adopted a rather aggressive approach towards technology and data intensive companies, the United States anti-trust authorities are seen acting with significant caution.

- As far back as 2008, the Department of Justice (**"DOJ"**) of the United States required Thomson to sell financial data and related assets in order to acquire Reuters
- The DOJ unsuccessfully opposed the merger between entertainment major Time Warner and the largest telecom provider AT&T, arguing that the merger would allow merged entity to have exclusive access to Time Warner's 'must have' television content to either raise its rivals' video programming costs or drive those same rivals' customers to AT&T's subsidiary DirecTV
- In Europe, in the Microsoft/LinkedIn merger, the European Commission (**"EC"**) had noted that although privacy concerns are covered under data protection laws, the same could be considered as a non-price competition factor in merger control assessments to the extent that consumers consider it as significant factor in the quality of the services offered
- The EC imposed a fine of USD 122 million on Facebook for failing to disclose that post its acquisition of WhatsApp, it would combine the data of the users of the two platforms
- The EU's Competition Commissioner Margrethe Vestager has recently promised to 'keep a close eye on how companies use data' and a number of European antitrust authorities have conducted full-blown studies on big data issues
- Anticompetitive effects of Apple's acquisition of music recognition app, Shazam is being investigated by the EC

The EC has imposed fines of USD 2.7 billion and USD 3.8 billion on Google with respect to certain conduct relating to its Shopping page and Android OS, respectively.

Technology companies in India: Understanding the ramifications under India's competition laws framework

Competition law in India is enforced primarily by the Competition Commission of India ("CCI"), established under the Competition Act, 2002 ("Act"). The CCI has the responsibility to "prevent practices having an adverse effect on competition and sustain competition in the market" and has been quite actively enforcing the Act since its inception in 2009.

Under the Act, the CCI can look into three aspects:

- Anti-competitive agreements, including collusive agreements between competitors under Section 3 of the Act
- Abuse of dominant position by an enterprise under Section 4 of the Act
- Regulation of mergers and acquisitions under Section 5 and 6 of the Act.

While there has been limited scrutiny by the CCI on issues relating to data, it has, in 2017-2018, passed three orders dealing with the impact and significance of data in the competition landscape which included complaints filed against WhatsApp and Google and approving the merger of Bayer and Monsanto.

It is noteworthy – and perhaps an indicator of the things to come – that in 2018, while approving the merger between Bayer and Monsanto, the CCI directed the merged entity to provide agricultural information/data on fair, reasonable and non-discriminatory terms.

Key concerns

Broadly speaking, the primary concerns that arise due to the interplay of data collection, processing and transfer, and competition law in the Indian context are identified here:

Collusive behaviour

Any technological platform enabling 'real-time' access to price and quantity data is viewed with suspicion by competition regulators

Possibility of collusion between competitors using a 3rd party developed algorithm or AI, which relies on data sets or 'real-time data'

This poses new & legal compliance challenges for the enterprises, diminishing the lines between permitted and prohibited conduct

Possibility of abuse

Any abuse of market power arising out of control over data may raise concerns such as:

- Access to data can be used to implement entry barriers against other participants in the market
- Discriminatory access to such data may also raise potential red flags
- Concerns may also arise from exclusive agreements if they prevent other entities from accessing data or foreclosing rivals' opportunities to procure similar data, by making it harder for consumers to adopt rival technologies or platforms

Big Data in Mergers

Competition authorities are likely to examine potential lessening of competition that may result from the acquisition of important data. A few reasons for this may be:

- The transaction combines substitutable datasets
- The transaction transfers control of critical data which impacts the existence of the acquiring firm's competitors and other players

If in the assessment of the competition authority, the acquisition is likely to substantially lessen competition in the market, it may direct divestiture of the data or direct compulsory licensing/access to the data on predetermined terms and conditions

CCI has the power to impose significant penalties, up to 10% of the average of the turnover for the last three years or in case of a cartel, 3 times of the profit for each year in continuation of a cartel. In case of an abuse of dominant position, the CCI can also direct division of an enterprise. Similarly, while assessing a merger, CCI can direct divestment of certain assets or pass detailed guidelines on carrying of certain business activities, where the merger is found to have or is likely to have adverse effect on competition in India.

Conclusion

Although, 'big data' has been the center of attention from competition regulators globally, the authorities are still in the process of gaining a better understanding of inherent issues and ascertaining the manner in which the traditional tools can be applied to a technology driven landscape. The vulnerability to competition law scrutiny as a result of data accumulation and processing, extends across sectors ranging from the obviously vulnerable businesses (such as, aggregators, social networks, search companies) to businesses in traditional sectors (hospitality, insurance, life sciences, etc.). It would be prudent for companies to follow basic hygiene measures, including a regular review of existing policies, practices and agreements pertaining to data collection /processing/access in order to identify possible competition compliance gaps and risks involved; seeking specialist advice on issues pertaining to M&A activity; ongoing negotiations with parties in relation to data collection; streamlining policies, practices and contracts with applicable legal requirements; etc.

Even though limited information and jurisprudence is available in India, given the nascent nature of competition laws framework in the country, it is quite possible to assess potential competition issues that can arise for technology and data-intensive companies in India, and recommend suitable measures to limit such potential regulatory risks. Pre-emptive risk assessment and proactive mitigation steps are indeed the need of the hour.

ECONOMIC LAWS PRACTICE
ADVOCATES & SOLICITORS

Mumbai

109 A, 1st Floor, Dalamal Towers
Free Press Journal Road, Nariman Point
Mumbai 400 021
T: +91 22 6636 7000

Delhi

801 A, 8th Floor, Konnectus Tower
Bhavbhuti Marg
New Delhi 110 001
T: +91 11 4152 8400

Ahmedabad

801, 8th Floor, Abhijeet III
Mithakali Six Road, Ellisbridge
Ahmedabad 380 006
T: +91 79 6605 4480/1

Pune

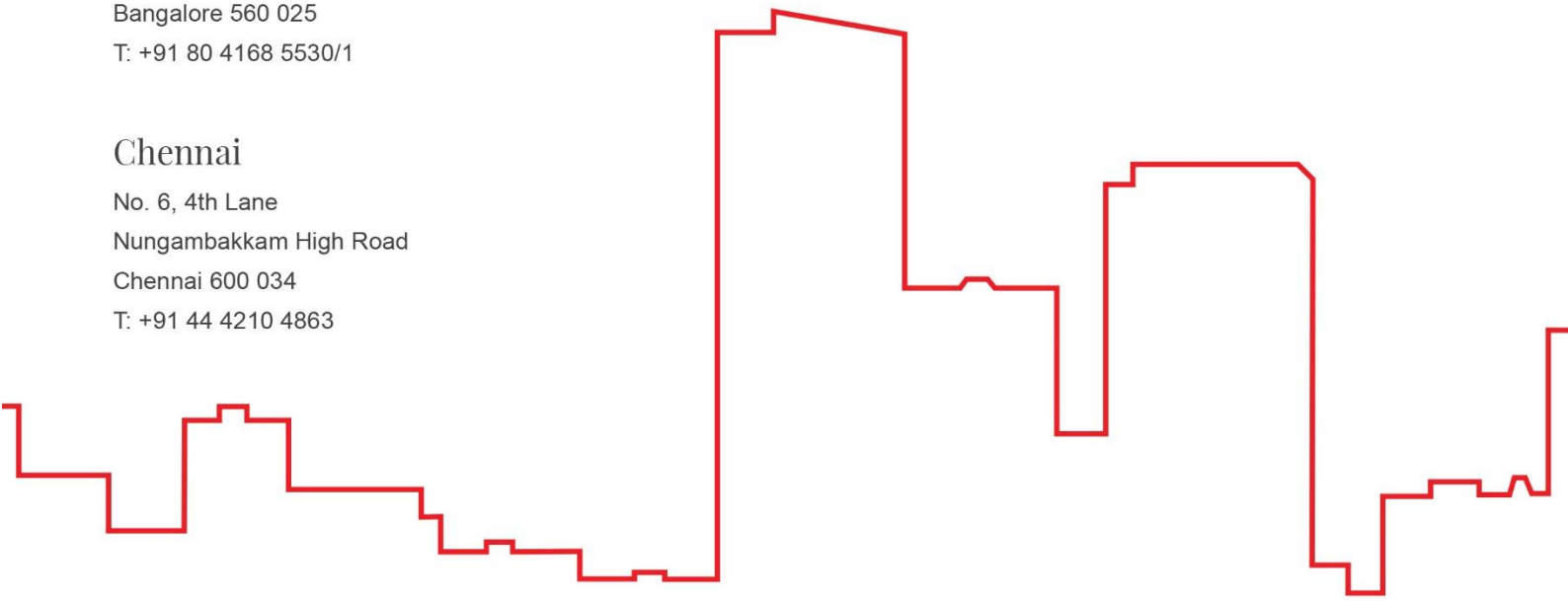
202, 2nd Floor, Vascon Eco Tower
Baner Pashan Road
Pune 411 045
T: +91 20 49127400

Bengaluru

6th Floor, Rockline Centre
54, Richmond Road
Bangalore 560 025
T: +91 80 4168 5530/1

Chennai

No. 6, 4th Lane
Nungambakkam High Road
Chennai 600 034
T: +91 44 4210 4863



Disclaimer:

elplaw@elp-in.com

elplaw.in **/elplaw.in** **/ELPIndia** **/company/economic-law-practice**