AI, Machine Learning & Big Data

2019

First Edition

Contributing Editors:
Matt Berkowitz and Joshua Thompson

global legal group

Global Legal Insights

AI, Machine Learning & Big Data

2019, First Edition
Contributing Editors: Matt Berkowitz & Joshua Thompson
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS - AI, MACHINE LEARNING & BIG DATA

2019, FIRST EDITION

Contributing Editors
Matt Berkowitz & Joshua Thompson, Shearman & Sterling LLP

Production Sub Editor
Amy Norton

Senior Editors
Caroline Collingwood
Rachel Williams

General Consulting Editor
Alan Falach

Publisher
Rory Smith

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Matt Berkowitz & Joshua Thompson for all of their assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-912509-79-9
ISSN 2632-7120

Printed and bound by CPI Group (UK) Ltd, Croydon, CR0 4YY
July 2019

CONTENTS

India

Priti Suri, Arya Tripathy & Janarth Visvanathan
PSA

1. Trends

1.1 India is marching forward to become a leading hub for innovation, research and development, with increased focus on digitisation and internet connectivity for its population of 1.3 billion. The internet economy is expected to contribute 7.5% to India's GDP by 2020[1] and the share of digital technology investment, such as artificial intelligence ("**AI**"), machine learning, cloud computing, Internet of Things ("**IoT**"), and other emerging technologies will rise from 35% in 2020 to 60% in 2025.[2]

1.2 *Trends in AI and machine learning*: Beyond the revenue and investment statistics, Indian companies registered promising numbers for foreign intellectual property ("**IP**") filings, with over 4,600 patents filed in the United States during 2015–2018, of which AI, cyber security, IoT and cloud computing accounted for over 50% in 2017.[3] More specifically, AI stands as the front runner in the emerging technology space, with over 300 patents, and machine learning was the leading sub-domain with a share of over 70%.[4] While AI has given Indian companies a dynamic foundation for expanding capabilities, big players are suspected to remain reluctant to shift from traditional practices; and as of 2017, only 22% of firms in sectors like banking and financial services, telecommunications, media and technology, manufacturing and retail, and healthcare services were utilising AI in their business processes.[5] The banking and financial sector leads the way, with AI utilisation in improving customer interaction, intelligent automation of back office operations, fraud analytics, credit score analysis, wealth management and risk prediction. The manufacturing sector has also implemented advanced robotics at scale, and a 2018 study revealed that 19% of Indian manufacturing companies are already using AI significantly, which places India 3rd in the world in this ranking.[6] In contrast to the conservative approach of most of the bigger companies, Indian start-ups in diverse sectors like education, agriculture, e-commerce, insurance, healthcare, banking and financial services, and automobiles are eager to design and implement their business models around AI and machine learning. This is evidenced from the fact that during 2015–2018, nearly 200 patents majorly focused on image processing, AI, cyber security, vehicle technology and IoT were filed in the United States by start-ups.[7]

1.3 *Trends in Big Data*: The Big Data and analytics market is rather promising for India, and Indian companies, big and small alike, are progressively becoming cognisant that a mature, advanced analytics strategy has a direct bearing on their business performances. The Big Data industry is estimated to generate US$ 2.03 billion annually at a 28.3% growth rate, with advanced analytics, predictive modelling and data science accounting for 12% and Big Data for 24%.[8] Most of the revenue earned from this industry is through service

exports to the United States (*60%*) and United Kingdom (*8.4%*).[9] The domestic market contributes up to 4%.[10] Several industry verticals such as banking and financial services, marketing, advertising, pharmaceuticals, healthcare, e-commerce, retail, telecoms, and travel and hospitality form the consumer base for this industry. While AI and machine learning may be settling in pace with Indian companies, Big Data and analytics have become sophisticated and are aggressively used by companies of all sizes and scales; this encouraging trend is likely to continue in the foreseeable future.

1.4 *Government's approach*: The Government of India ("**GOI**") acknowledges the potential market disruption that can ensue from AI, machine learning and Big Data, and has been eager to institute a policy framework in order to maximise the positive impact. Towards this, GOI's interim budget for 2019 proposes allocation of about US$ 57.4 million for setting up a National Centre on AI, a national AI portal and 20 institutes of eminence for research and innovation.[11] The Ministry of Commerce & Industry constituted a Task Force on AI for India's Economic Transformation, which published its report in March 2018 ("**GOI Report**"). Subsequently, in June 2018, "*NITI Aayog*", GOI's policy think tank, published a Discussion Paper on the National Strategy for AI ("**Niti Aayog Paper**") which sets *#AIforAll* as the theme to boost AI outreach to general public. Both of these documents analyse the state of AI in India, recommend steps required for the development and utilisation of AI, such as setting up dedicated inter-ministerial funds for AI-related activities, creating digital data banks, marketplaces and exchanges, and global participation in developing standards for AI systems. These reports identify healthcare, agriculture, education, infrastructure, transport, retail, accessibility, technology, environment, smart cities, national security and public utility services as the sectors of relevance in India for AI. They have also recognised the lack of Big Data and access, which is required for AI development, deeming it necessary that GOI builds a large corpus of data across domains, including through collaboration with private organisations.

At the same time, the surge in the use of AI and Big Data has stoked worries that only big businesses with resources will be able to harness their benefits, leaving the smaller players behind. This largely stems from ownership and access issues of data and technologies. Towards this, GOI's National Data Sharing and Accessibility Policy ("**NDSAP**"), which provides businesses with access to a wide variety of scientific and technical data collected by GOI, as well as the Open Government Data Platform India – which was created to provide single-point access to governmental data sets – shall help create a level playing field.

1.5 *AI defence projects*: Taking note of the GOI Report, on January 2, 2019, the Ministry of Defence sanctioned two projects.[12] *Firstly*, US$ 10.6 million has been sanctioned for the Centre for Artificial Intelligence and Robotics, a laboratory under GOI's Defence Research and Development Organization, for developing signal intelligence solutions for enhancing armed forces' intelligence and analysis capabilities. *Secondly*, US$ 258,723 has been sanctioned for the project "*Energy Harvesting Based Infrared Sensor Network for Automated Human Intrusion Detection*", deriving solutions based on IoT principles. This is a modest start, but is testimony to GOI's intent of adopting emerging technologies and AI for improving capabilities in defence and national security.

1.6 *Data protection & privacy*: On the other hand, Indians are becoming increasingly wary of informational privacy and the absence of a robust data protection regime. As per a 2018 survey regarding AI conducted with industry stakeholders, 93% expressed concerns regarding data privacy.[13] 2018 was a particularly eventful year in India for data protection and privacy. The Indian Supreme Court ("**SC**") in *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*[14]

recognised the right to privacy including informational privacy both as a constitutionally protected fundamental right enforceable against the state, and as a horizontal right enforceable against private parties, and emphasised the need for thorough data protection laws. Consequently, the Ministry of Electronics and Information Technology published the draft Personal Data Protection Bill, 2018 ("**PDP Bill**"). The PDP Bill will have extraterritorial effect, and is significantly influenced by the European Union General Data Protection Regulation ("**EU GDPR**"), proposing the establishment of a Data Protection Authority, stricter principles, and conditions and compliance requirements for processing personal data. It also provides for substantial penalties and imposes personal liability on corporate officers for breaches. The PDP Bill is likely to be placed before the Parliament for legislative approval in July 2019, and if implemented in its current form, will require organisations using personal data for their internal and external functionalities to completely overhaul their practices and policies.

1.7 *Localisation trend*: Further, there is a larger policy trend to seek data localisation in India. The PDP Bill seeks to implement myriad localisation requirements, where certain categories of sensitive personal data will be notified as "*critical*" and can only be stored and processed in India, whereas other kinds of personal data can be transferred out of India, provided that a serving copy is stored in India. Similarly, the Reserve Bank of India ("**RBI**") issued a notification in April 2018 directing payment system providers to store all payment systems-related data within India. Furthermore, the Draft National e-Commerce Policy proposes data localisation in several e-commerce categories in order to facilitate the collection and sharing of data exclusively in India. While data protection, access rights and national security seem to be the underlying ideology for localisation, stakeholders have voiced concerns on the adverse impact that it may cause for the booming Big Data and AI industry in India. Undoubtedly, it will be worthwhile to witness how the evolving data protection regime is finally shaped, whether it balances conflicting stakeholder interests and how businesses adapt to the changed regime.

2. Ownership/protection

2.1 *AI algorithm ownership*: Algorithms are protected as "*literary works*" under the Copyright Act, 1957. Literary works include computer programs, tables, compilations and computer databases. To copyright an AI algorithm, the applicant must prove that the AI algorithm is original. Upon the successful registration of AI algorithms, the ownership vests with the author, i.e. the person who causes such algorithm to be created and applies for a copyright. Irrespective of copyright registration, AI algorithm expression is protected under the author's common law rights to claim authorship and compensation for any distortion, mutilation, modification or act that prejudices his honour or reputation. Where the author creates the algorithm under a contract of service or apprenticeship, the ownership will vest with the employer, unless there is an agreement to the contrary.

While AI algorithms standalone are excluded from patent protection under the Patents Act, 1970 ("**Patents Act**"), they can be patented if they satisfy the criteria of "*computer related inventions*" provided under the Guidelines for Examination of Computer Related Inventions issued by the Office of the Controller General of Patents, Designs and Trademarks. As per these Guidelines, an algorithm is patentable when it includes a "*novel hardware component*" and has a "*technical effect*" or a solution to a technical problem, resulting in a technical advancement that did not exist in prior art. The requirement of a novel hardware component with new technical effect has been an impediment to the patentability of AI algorithm-based inventions, with most patent applications being refused on this basis.

2.2 *AI ownership issues*: Copyright protection will only safeguard the original expression of the AI algorithm and not the functional aspects thereof, including subsequent versions if they lack substantive variation from the original version, the AI product and its supporting hardware, and AI-generated works. As discussed above, AI technology is extremely unlikely to be registered as patents. Consequently, mere copyright protection of the original AI algorithm will not be adequate for entities seeking to safeguard their commercial and intellectual interests in the entire AI product/service and its variations, which can be utilised by a third party without necessary licensing or assignment arrangements with the author. Further, ownership of AI-based inventions without human intervention under Indian law is a grey area. Section 6 of the Patents Act allows only the "*true and first inventor*" to make a patent application. "*True and first inventor*" is defined in an exclusionary manner with no specific requirement for the inventor to be a natural person.[15] This suggests that legal persons can apply for patents. However, Indian law does not recognise AI as a legal person and so AI *per se* cannot qualify as the "*true and first inventor*". Until such time as AI is granted personhood, the ownership of AI-based inventions will remain a murky area.

2.3 *Practices followed*: According to a WIPO report, India ranks 3rd and 4th for scientific publications in fuzzy logic and machine learning, and 8th or lower for patent filing activity in both these areas owing to the difficulty in obtaining patents for AI and AI-based inventions in India.[16] Despite these limitations, India has seen rapid growth in AI research. As per the said WIPO report, India ranks highly in publications in various areas of AI functional applications, such as computer vision, natural language processing, distributed AI, planning and scheduling, speech processing, and predictive analysis. Unfortunately, this has not translated into patenting activity on a similar or comparable scale. As an alternative, Indian companies are seeking patent registration and other IP protection in foreign jurisdictions that provide more conducive AI ownership framework. In the given scenario, Indian AI companies retain AI technology, innovations and developments as trade secrets, know-how and confidential information, thereby extensively relying on contractual safeguards and indemnifications while dealing with third parties.

2.4 *Data ownership, security & information privacy*: Data processing and protection is currently governed by the Information Technology Act, 2000 ("**IT Act**") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**IT Rules**"). The IT Rules contain the procedural and substantive data protection obligations concerning collection, receipt, possession, storage, or any other manner of dealing or handling of personal information. "*Personal information*" is any information relating to a natural person, which directly or indirectly in combination with other information can lead to a natural person's identification. Certain kinds of personal information such as passwords, financial information, physical, physiological and mental health conditions, medical records, biometric information, and sexual orientation are treated as sensitive personal data. As per the IT Rules, personal information can be processed by obtaining consent from the concerned individual or under a lawful contract. However, there is no express legislative, regulatory or judicial principle that clarifies the issues of data ownership in India.

Nonetheless, as discussed in paragraph 1.6 above, the SC has recognised informational privacy as an individual's fundamental and legal right. It explains informational privacy as the control one has over the access and sharing of their information, but this exposition falls short in settling the principle of data ownership with the concerned individual conclusively. The PDP Bill seeks to establish a fiduciary and trust relationship between the person(s) that

determines the purpose and means of processing personal information, i.e., the data fiduciary (*equivalent of the controller under EU GDPR*), and the concerned individual whose information is processed, i.e. the data principal (*equivalent to the data subject under EU GDPR*). For this fiduciary relationship, the PDP Bill supposes that the data fiduciary is in a position to ascertain the best interests of the data principal, and must accordingly process personal information in such manner that does not cause harm to the data principal. While common law jurisprudence in India settles the principles for a traditional fiduciary relationship, liability questions in a fiduciary matrix are fact-specific and cannot be contained in a strait-jacket formula. Hence, when the PDP Bill is enacted, the application of conventional fiduciary principles to data stakeholders will call for abundant caution.

3. Antitrust/competition laws

3.1 The Competition Act, 2002 and rules made thereunder ("**Competition Act**") govern market competition in India, and are enforced by the Competition Commission of India ("**CCI**"). The Act prohibits (i) anti-competitive agreements causing or which are likely to cause appreciable adverse effect on competition,[17] (ii) abuse of dominant position,[18] and (iii) certain kinds of mergers or amalgamations between entities where antitrust concerns can arise.[19] AI and Big Data can raise potential risks to market competition with the use of sophisticated pricing algorithms, asymmetrical access to data, technological collusion, and new forms of entry barriers.

3.2 CCI is active in scrutinising AI and Big Data-enabled businesses, and liability can be affixed on corporate entities for any direct or indirect collusion that results in appreciable adverse effect on competition through anti-competitive agreements, mergers, or by abuse of dominance. For instance, in the *Bayer/Monsanto merger notification*, CCI recognised that the merger between Monsanto and Bayer's existing genome editing and Big Data technologies would give them a significant competitive edge.[20] While CCI allowed the merger on the ground that a competitive edge *per se* does not constitute an anti-competitive practice, this indicates that mergers between AI and Big Data players are being scrutinised by CCI for pre-merger approvals. The exploitation of data for gaining a competitive edge is not prohibited *per se*, but AI and Big Data businesses must comply with competition law, failing which antitrust concerns are likely to arise. Similarly, CCI fined Google US$ 19.5 million for "*search bias*" that is tantamount to abuse of dominant position in the market.[21] Google was found to give preference to its commercial flight search function in the search results page, disallowing fair access to its rival's product by giving it a lower search result ranking. It was held that Google had used its dominance in the market for online general web searches to push restrictive conditions, thereby violating antitrust principles. This illustrates a scenario where Google used its algorithm for foreclosure of competition. While in Google's case, the algorithm was designed to foreclose competition, there could be situations where autonomous and self-learning AI algorithms, even without specific instruction or designing, could tacitly collude or engage in anti-competitive practices, like price fixing, bid rigging, etc., in which case it is likely that CCI will initiate investigations. However, the attribution of liability in case of autonomous AI is a grey area, and is dealt with in paragraph 6 below.

4. Board of directors/governance

4.1 *Current trend*: A 2018 survey indicates that nearly 87% of global CEOs are proactively investing in cyber security and shaping their governance policies, whereas less than 50% of participating Indian CEOs have put any such measures in place.[22] Most Indian companies

in compliance with the IT Act and IT Rules have instituted reasonable organisational, managerial, technical, operational and physical information security measures. Bigger IT/ITES companies opt for global standards and implement IS/ISO/IEC 27001: Information Technology – Security Techniques Information Security Management System – Requirements. Further, companies dealing with information technology and personal information are legally obligated to put in place detailed terms of use and privacy policies, and appoint designated officers as grievance officers to resolve any complaints. The primary focus underlying these processes is to operate a personal information management system that complies with the minimal legal requirements under the IT Act; however, it cannot be said with certainty that a privacy governance framework is one of the key agenda items for Indian boards.

4.2 *Proposed change*: This trend will undergo a complete change when the PDP Bill gets notified, which essentially mandates data fiduciaries to ensure that managerial, organisational business practices and technical systems are designed to protect informational privacy. The PDP Bill proposes obligations on data fiduciaries to abide with principles of lawful, fair and reasonable processing, purpose, collection and storage limitations, and retain data quality throughout its lifecycle. All of these principles shall form the underlying basis of data processing and will have wide ramifications, with breaches being dealt with on a case-to-case basis. The PDP Bill also requires data fiduciaries to set up internal systems and processes for honouring the data principal's right to access and confirmation, and correction requests. Further, certain data fiduciaries that will be notified by the Data Protection Authority as "*significant data fiduciaries*" shall be obligated to conduct data protection impact assessments, appoint a Data Protection Officer, conduct periodic data audits, and maintain processing records. Hence, the PDP Bill will require boards of AI and Big Data companies to align business practices and processes around a privacy governance framework that views privacy as the default setting, embeds privacy into design, takes a user-centric approach, enables full lifecycle protection, is proactive towards breach scenarios, is transparent and accountable, and is not limited to personal information management systems.

4.3 *Fiduciary duties, governance and impact*: While the IT Act is silent on duties that AI and Big Data companies' boards of directors must discharge for data protection and privacy, Section 166 of the Indian Companies Act, 2013 ("**Companies Act**") imposes statutory fiduciary duties on directors. These duties, *inter alia*, obligate directors to (i) act in good faith to promote the objects of the company for the benefit of members as a whole, and in the best interests of the company, its employees, shareholders, community, and protection of the environment, (ii) exercise their duties with due and reasonable care, skill and diligence with independent judgment, (iii) steer clear of direct or indirect conflicts of interest with the company, (iv) not achieve or attempt to achieve any undue gain or advantage personally or for his relatives, partners or associates, and (v) not assign their office. Further, Section 134 of the Companies Act requires the board to provide a statement indicating development and implementation of a "*risk management policy*" that identifies the risk elements which, in the board's opinion, may threaten the existence of the company. It also requires directors to provide a "*directors' responsibility statement*", *inter alia*, certifying that directors had devised proposed systems to ensure compliance with applicable laws, and that those systems were adequate and operating effectively. Failure to comply with the aforestated obligations entails a monetary fine between approximately US$ 1,400–35,900 and/or imprisonment. Whether a director has complied with the obligations shall be proved on facts as evidenced in corporate records, filings, minutes of meetings, annual reports, notes of dissent, corporate registers and other correspondence.

Apart from these duties, India's securities and stock exchange regulator, the Securities and Exchange Board of India ("**SEBI**"), constituted the "*Kotak Committee*" in June 2017 to review and make recommendations on existing corporate governance standards and practices in India. The committee published its report in October 2017, pursuant to which revised corporate governance obligations were imposed on listed companies. In terms of protecting shareholder interests, the Kotak Committee recognises the risk sub-committee of listed companies as the core safeguarding committee. It recommended SEBI to revamp governance standards so that the risk and technology sub-committees of boards must pay particular attention to cyber security concerns, include cyber security within their scope of duties, and increase the periodicity of technical internal reviews. Subsequently, SEBI has required the committees of the top 500 listed companies to include cyber security and related risks as part of their role.

Based on the perusal of the abovementioned obligations, it can be concluded that the scope of the director's fiduciary duties and good governance measures are far reaching and not circumscribed to corporate and legal compliances. The nature of these obligations requires directors of AI and Big Data companies to exercise a duty of care and diligence and exercise independent judgment, while strategising and planning business operations, remaining abreast of evolving legal requirements, monitoring and supervising organisational data processing and protection practices including data breaches, mitigating steps undertaken, and implementing innovative governance frameworks that balance business interests with the individual's reasonable expectation of privacy.

5. Regulations/government intervention

5.1 *Current legal framework*: Currently, India does not have specific laws catering to the regulation of AI, machine learning and Big Data. As previously discussed in paragraph 2.4 above, the IT Act and IT Rules contain the procedural and substantive data protection obligations concerning the collection, receipt, possession, storage, or any other manner of dealing with personal information. AI, machine learning and Big Data companies must comply with the requirements prescribed under the IT Act, other delegated legislation made thereunder and the IT Rules for their operations. Some of the key provisions under the IT Act pertain to consent or a lawful contract as the basis for processing personal information, implementing privacy policies, adoption of reasonable organisational and technical security measures, pre-requisites for cross-border data transfer, intermediary liabilities,[23] manner of encryption and decryption and monitoring publication of online content.

Non-compliance and breach can entail a penalty, liability in compensation and personal liability for the person in charge of business activities (*directors, data protection officers*), particularly for (i) negligence or failure to maintain and implement reasonable security practices, thereby resulting in wrongful gain or loss to another, (ii) disclosure of personal information where it is not necessary for the purposes or without appropriate consent, and (iii) publication, transmission or facilitation thereof of any obscene or sexually explicit content by an intermediary in certain instances. Complaints can be lodged as criminal offences with cyber crime cells of respective regional police departments and are adjudicated by criminal courts. Civil complaints are reported and adjudicated by IT Secretaries of each state's Ministry of Information Technology. Additionally, claims for compensation on account of breach of confidentiality and privacy can be filed in civil courts. Based on official records available for 2013, it is more likely that an aggrieved individual will file a criminal complaint with a cyber cell than a civil complaint with the Ministry of Information Technology.[24]

5.2 *Developments*: However, as elaborated in paragraphs 1.6, 2.4 and 4.2 above, the legal regime around data protection and privacy is undergoing a sea change. Even though data protection is greatly prioritised, regulatory framework for AI, machine learning and Big Data is yet to be examined in detail. The GOI Report and Niti Aayog Paper dealt with in paragraph 1.4 above are the first steps towards creating dedicated AI and Big Data policies, and are crucial for the development of comprehensive legal frameworks. It is noteworthy that GOI is quickly adopting AI and Big Data for departmental functionalities. One of the Kotak Committee's recommendations to strengthen corporate governance practices in India, referred to in paragraph 4.3 above, is for SEBI to create a separate department that implements a robust data processing framework and make use of data analytics and AI tools to detect fraudulent financial and corporate reporting. In a similar vein, the Ministry of Corporate Affairs has indicated that AI will be integrated in their online portal utilised for statutory fillings and corporate information dissemination to the general public. The Ministry also intends to interlink various government databases by 2021–2022, including income tax, goods and services taxes, RBI, and financial intelligence unit databases.

6. Liability

6.1 The Indian legal framework does not vest AI with legal personality. Accordingly, AI does not have the power to acquire, hold and dispose of property, enter into contracts, sue and be sued independently, and be held liable for civil claims and criminal offences.

6.2 However, the use of AI may entail civil liability for manufacturers or sellers of AI products and enabled services under the Consumer Protection Act, 1986 (*in the nature of defective goods and deficiency of services*), the IT Act (*as discussed in paragraph 5.1 above*), tortuous claims for negligence, or contractual claims. For example, civil, tortuous and/or contractual liability may arise if AI performs defective services, is negligent, fails to protect confidential or personal information, or causes harm to the end user through malfunctioning. While the theoretical possibilities of these civil claims remain, to date there is no Indian jurisprudence. How traditional civil, tortuous and contractual liability principles will apply when a claim's cause of action relates to AI is a grey area. The issue becomes even more contentious where criminal liability is sought to be imposed on AI. The governing law is contained in the Indian Penal Code, 1860, which requires the twin conditions of guilty act (*actus reus*) and mind (*mens rea*) to be proved beyond reasonable doubt for attributing liability. Assuming that AI is granted personhood in future, it will be difficult to apply criminal liability principles as applied to legal entities (*i.e. mens rea is substantiated by proving guilty mind of the controlling natural persons*) in the context of autonomous and semi-autonomous AI. In light of these uncertainties, it is imperative that the evolution of the regulatory framework specifically focus on and clarify the liability principles for AI and machine learning.

* * *

Endnotes

1. NASSCOM "*India on track to be a trillion dollar digital economy*" [2019] available at https://www.nasscom.in/interviews/india-track-be-trillion-dollar-digital-economy?width=960px&inline=true#colorbox-inline-1678126235 (last accessed on April 4, 2019).

2. NASSCOM "*Perspective 2025 Report*" [2017] available at https://www.nasscom.in/interviews/imperatives-digital-ready-india?width=960px&inline=true#colorbox-inline-1011911476 (last accessed on April 4, 2019).
3. NASSCOM "*Emerging Technologies: Leading the next wave of IP creation for India*" [2019] available at https://community.nasscom.in/communities/policy-advocacy/emerging-technologies-leading-the-next-wave-of-ip-creation-for-india.html (last accessed on April 4, 2019).
4. *Ibid.*
5. Nishant Bansal, Shalil Gupta & Sandeep Sharma "*Artificial Intelligence In Indian Enterprises: Preparing For The Future*" [2017] available at https://www.intel.ai/wp-content/uploads/sites/53/2018/04/IDC_Whitepaper_AI-in-India_FINAL.pdf (last accessed on April 4, 2019).
6. The Boston Consulting Group "*AI in the Factory of the Future*" [2018] available at http://image-src.bcg.com/Images/BCG-AI-in-the-Factory-of-the-Future-Apr-2018_tcm108-188454_tcm9-188767.pdf (last accessed on April 4, 2019).
7. *Supra* note iii.
8. Analytics India Magazine & Analytixlabs "*Analytics India Industry Study 2017*" [2017] available at https://analyticsindiamag.com/wp-content/uploads/2017/07/Analytics-India-Industry-Study-2017.pdf (last accessed on April 4, 2019).
9. *Ibid.*
10. *Ibid.*
11. Hindustan Times "*Budget 2019: Govt plans to push AI with national centre, allots Rs 400 crore*" [2019] available at https://www.hindustantimes.com/budget/budget-2019-govt-plans-ai-push-with-national-centre/story-fdqlbqfOZMdruQ5GxEaU6M.html (last accessed on April 4, 2019).
12. Ministry of Defence press release "*Artificial Intelligence*" [2019] available at http://pib.nic.in/newsite/PrintRelease.aspx?relid=187044 (last accessed on April 4, 2019).
13. PricewaterhouseCoopers "*Artificial intelligence in India – hype or reality*" [2018] available at https://www.pwc.in/assets/pdfs/consulting/technology/data-and-analytics/artificial-intelligence-in-india-hype-or-reality/artificial-intelligence-in-india-hype-or-reality.pdf (last accessed on April 4, 2019).
14. (2017) 10 SCC 1.
15. Section 2(1)(y) of Patents Act, 1970 defines "*true and first inventor*" to not include either the first importer of an invention into India or a person to whom an invention is first communicated from outside India.
16. WIPO "*WIPO Technology Trends 2019 – Artificial Intelligence*" [2019] available at https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf (last accessed on April 4, 2019).
17. Section 3 of the Competition Act prohibits any agreement in respect of production, supply, distribution, storage, acquisition, or control of goods or provision of services which causes or is likely to cause an appreciable adverse effect on competition, such as cartels, bid rigging, and certain kinds of vertical agreements.

18. Section 4 of the Competition Act prohibits a dominant entity from abusing its market position, such as directly or indirectly imposing unfair/discriminatory conditions for purchase/sale of goods or services, discriminatory pricing, limiting/restricting production of goods, denying market access, etc.
19. Section 6 of the Competition Act lays out the threshold criteria when combinations are scrutinised for antitrust concerns and factors such as entry barriers, likelihood of profit increase, actual impact on competition in the relevant market and the degree of countervailing power in the market are taken into consideration.
20. Combination Registration No. C-2017/08/523, dated June 14, 2018.
21. *In re: Matrimony.com Ltd. and Google LLC*, case nos. 07 and 30 of 2012, decided on February 8, 2018.
22. PricewaterhouseCoopers, "*Privacy in the data economy*" [2018] available at https://www.pwc.in/assets/pdfs/publications/2018/privacy-in-the-data-economy.pdf (last accessed on April 4, 2019).
23. Section 2(1)(w) of the IT Act defines an "intermediary" as any person who on behalf of another person receives, stores or transmits electronic records or provides any service with respect to such records.
24. As per official records available for 2013, 93 complaints for breach of privacy and confidentiality, 27 for unauthorised access and 1,228 for publication and transmission of obscene content were filed across different cyber crime cells across India; refer to the Government report "*Cases registered under IT Act of Cyber crime during 2013*" available at https://data.gov.in/catalog/cases-registered-under-it-act-cyber-crime (last accessed on April 4, 2019); statistics beyond 2013 are not available.

Priti Suri
Tel: +91 11 4350 0500 ext 501 / Email: p.suri@psalegal.com

Priti Suri, Founder and Managing Partner, is a seasoned lawyer with over 32 years' experience. A first-generational business lawyer who set up and developed the firm, her global experience provided valuable insights and she is known for her pragmatic ability to get the deal done. Priti became the first Asian to be honoured with the prestigious "*Mayre Rasmussen Award*" by the American Bar Association ("**ABA**"). The *Indian Business Law Journal* has consecutively rated her as one of India's top 100 lawyers, and the International Council for Commercial Arbitration also listed her amongst the top 100 corporate advisers. Priti is currently on the Board of ITechLaw and is the Vice-Chair of Inter-Pacific Bar Association's Publications Committee. She has chaired the India Committee of the ABA's Section of International Law.

Arya Tripathy
Tel: +91 11 4350 0500 ext 521 / Email: a.tripathy@psalegal.com

Arya Tripathy, Principal Associate, has eight years of experience in advising various domestic and international clients on diverse aspects of business and commercial law. She focuses on advising clients in industry-specific practice areas like healthcare, pharmaceuticals, defence, IT/ITES, technology & media, automobiles, heavy manufacturing industries, and education. She has substantial experience in advising global and national clients on the evolving aspects of the data protection and privacy rights regime, with specific focus on the EU and Indian legal landscape, helping them navigate and create robust organisational data management and lifecycle processes. She has conducted data protection training for leading IT/ITES multi-national companies, organised round table sessions and spoken at public forums on comparative data protection jurisprudence. Arya proactively contributes to the firm's *pro bono* services and has advised several well-known clients, as well as emerging not-for-profit clients.

Janarth Visvanathan
Tel: +91 11 4350 0500 ext 516 / Email: j.visvanathan@psalegal.com

Janarth Visvanathan is an Associate at PSA. He practises corporate and commercial, M&A, trade, intellectual property, real estate, and data privacy laws. He regularly advises clients in the healthcare, e-commerce, and technology space. He graduated from Hidayatullah National Law University in 2016 and was admitted to the Bar in 2017.

PSA

14A & B, Hansalaya, 15 Barakhamba Road, New Delhi – 110001, India
Tel: +91 11 4350 0500 / URL: www.psalegal.com

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Blockchain & Cryptocurrency Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Commercial Real Estate**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fintech**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Strategic partner: