Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2024

Definitive global law guides offering comparative analysis from top-ranked lawyers

India: Law and Practice

Dhruv Singh, Shivalik Chandan, Arjun Khurana and Srijoy Das
G&W Legal

INDIA

Law and Practice

Contributed by:
Dhruv Singh, Shivalik Chandan, Arjun Khurana and Srijoy Das
G&W Legal

Contents

G&W Legal is a full-service business law firm that assists its clients at the intersection of law and pragmatism by combining the experience of big-law with the expertise of a boutique. The firm's attorneys advise and assist clients across intersecting areas such as corporate law, intellectual property, franchising and distribution, advertising and marketing, privacy and data protection, product liability and consumer protection, international trade, foreign investment, antitrust/competition, regulatory affairs, and dispute resolution. G&W Legal's TMT practice team has extensive experience in handling cross-border technology transactions, intricate licensing agreements, delicate data protection issues, fintech, platforms and intermediary regulations/liability, trust and safety, internet and social media, e-sports, and online gaming. The team handles all facets of data protection and privacy, traditional and new media, and digital business.

Authors

Dhruv Singh is counsel and head of G&W Legal's regulatory practice. With a wealth of experience working in-house with some of the biggest brands in the world, such as ByteDance (TikTok), Walmart-Flipkart and Penguin RandomHouse, Dhruv uses his business-side experience as well as legal subject-matter expertise to counsel large multinationals as well as individuals and non-profits on the ever-changing privacy and data protection regulations in India, digital media and intermediary regulations, technology transactions, AI products, content moderation and a host of other issues. Dhruv holds a CIPP-E certification from the International Association of Privacy Professionals and is a certified DPO.

Shivalik Chandan is an associate at G&W Legal. He has a particular interest in tech and media law, including on issues of freedom of speech. He regularly advises on issues of intermediary safe harbour, privacy, and data protection, as well as franchising matters.

Arjun Khurana is a partner at G&W Legal. He chairs the Tech, Media and IP practice, leading on emerging issues and dispute resolution. His practice traverses privacy and data protection, emerging issues, advertising and marketing, and digital businesses, with an additional focus on dispute resolution. Arjun is a member of the International Association of Privacy Professionals and INTA's Data Protection Committee.

Srijoy Das is counsel and an integral part of G&W Legal's TMT practice. He has over 27 years of experience advising multinationals expanding to and doing business in India. He is primarily responsible for the firm's Technology Transactions practice and has led teams for over 100 acquisitions in the technology sector. Srijoy has been appointed as a director by several Indian subsidiaries of large multinationals, including Bunnings Technologies India Private Limited (subsidiary of Wesfarmers Group, Australia), Fischer Systems India Private Limited (subsidiary of Fischer International, US) and Digi-Key Electronics & Automation Trading Private Limited (subsidiary of Digi-Key Corporation, US).

G & W Legal

C-9 / 9624,
Vasant Kunj
New Delhi
110070
India

Tel: +91 124 4402666
Email: srijoydas@gnwlegal.com
Web: www.gnwlegal.com

1. Metaverse

1.1 Laws and Regulation

As is the case with the laws of most other countries, there are no specific Indian laws designed to deal with the metaverse. In fact, the metaverse finds no mention and has not been defined under any Indian statute. The following regulations stand out as some of the most important from an Indian perspective.

Intellectual Property

- Trade marks – Trade marks may be used to protect branding and logos of brand owners from unauthorised use over the metaverse. While no cases of note have been reported in India, this is a topic that is currently getting a lot of attention. Brand-owners may consider it advisable to ensure that their interests in the virtual world are protected by way of their trade mark registrations.
- Copyright and personality rights – Indian copyright law potentially has the capacity to be enforced for infringements in the metaverse, as well as to protect programmes.

In an interesting case before the Honourable High Court of Delhi in 2023 (Digital Collectibles Pte Ltd. and Ors. v Galactus Funware Technology), the issue of the use of personality/image rights of sports players on NFTs without authorisation was dealt with in an attempt to obtain an injunction on the grounds of passing off, unfair competition, breach of personality rights, unjust enrichment and tortious interference with economic interests. In this instance, the prayer for an injunction was refused, citing it as unjust, and against the balance of convenience in the circumstances of the case.

Privacy

Pursuant to 2017's landmark judgment of the Supreme Court in Justice K.S. Puttaswamy v Union of India, the right to privacy has been guaranteed under the Indian Constitution. This means it may be enforced against the state. However, when it comes to private parties, it is still governed by statutes such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "SPDI Rules"), which are set to be replaced soon by the Digital Personal Data Protection Act, 2023 (DPDPA).

While the SPDI rules only require consent for the purposes of processing sensitive personal data such as sexual orientation, health data, biometrics, financial information and passwords, the DPDPA allows the processing of all personal data (not merely sensitive personal data) only on the receipt of consent of the data subject, or without consent in the event of a very limited range of legitimate purposes – such as for the purposes of responding to a medical emergency, or for the purposes of the state's performance of its obligations in furtherance of protecting sovereignty and integrity. Exactly how this is expected to play out will only become clear after subordinate legislation is published by the Indian government, which is expected later in 2024.

Intermediary Guidelines

Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Guidelines"), intermediaries, such as app service providers, are required to comply with its provisions to be able to use their status as an intermediary as a shield against being held personally liable for illegalities perpetrated by users on their platforms. The Intermediary Guidelines place a number of diligence obligations on the intermediary,

including the need to publish user agreements and the platforms' rules and privacy policies in a comprehensible and easily accessible manner, appoint a grievance officer, put together a grievance redressal mechanism, etc.

Free Speech

As with any other form of mass communication, the metaverse is also subject to the same Indian laws as applicable to more conventional means of communication. Where it doesn't act as an intermediary, the platform would be subject to the same laws on obscenity, defamation, sedition, and hurting of religious sentiment as a normal conventional platform, such as a news channel or a magazine.

2. Digital Economy

2.1 Key Challenges

The primary areas of legislation applicable to the digital economy in India are those of data protection and consumer protection, as well as the regulatory framework for digital payments. Additionally, as discussed below, the digital economy space has seen increased scrutiny by India's antitrust regulator in the past few years.

The SPDI Rules and requirements thereunder will be applicable on all aspects of the digital economy pertaining to personal data, such as the requirement of publishing a privacy policy, consent for "sensitive" personal data, purpose limitation and data minimisation. Similarly, the DPDPA, once put into force, will also apply to all entities (whether Indian or foreign) if they are processing personal data in India or if they are pursuing personal data of Indian data subjects with an intent of offering goods/services to them.

In 2019, India's primary consumer protection legislation, the Consumer Protection Act (CPA) was amended to explicitly include e-commerce consumers within its ambit. In furtherance of extending consumer protections to the digital economy, India has also put in place specific rules which are applicable to e-commerce sellers, which has placed obligations such as a specific restriction on utilising unfair trade practices, putting in place a grievance redressal mechanism, labelling and information obligations on the website, and a restriction on cancellation charges. These rules, in addition to being applicable on e-commerce entities incorporated in India, are also applicable on foreign entities which "systematically" offer goods/services to consumers in India.

In addition to the above, the Indian government has also issued guidelines regarding the restriction of false or misleading advertisements. These guidelines regarding advertisements place specific restrictions on advertisers and advertising agencies as well as manufacturers, sellers, and traders – specific conditions have been prescribed for an advertisement to be considered non-misleading. Additionally, conditions to be met for a "bait" advertisement to be valid have also been prescribed, and surrogate advertising has been prohibited.

In 2023, a set of guidelines was published by the government which restricted e-commerce entities from using dark patterns on their website. These guidelines prescribe 13 specific "dark patterns" and prohibit all platforms which systematically offer goods/services in India, advertisers, and sellers from engaging in any of these specified dark patterns. The dark patterns listed under the guidelines include false urgency, basket sneaking, forced action, bait and switch, and drip pricing.

Entities functioning as payment systems are bound to comply with a host of regulations issued by the RBI. The Payment and Settlement Systems Act (the "PSS Act") is the primary legislation governing payment systems in the country and prescribes that any payment system must be approved by the RBI prior to operating in India. The RBI is also empowered to issue regulations which payment systems are bound to comply with.

Additional guidelines relevant to payment systems include the Guidelines on Regulation of Payment Aggregators and Payment Gateways, the Master Direction on Credit Card and Debit Card – Issuance and Conduct Directions, and the circular on Tokenisation of Card Transactions. These guidelines and directions govern various disparate aspects of the digital payment economy in India and their relevance must be considered on a case-to-case basis, depending upon the nature of business of the entity.

Large e-commerce entities have been subject to increased scrutiny in terms of antitrust issues over the past few years. In 2020, the Competition Commission of India (CCI), the country's antitrust regulator, initiated a probe into Amazon and Flipkart, the two largest e-commerce platforms in the country, for alleged contraventions of the Competition Act, 2002 (the "Competition Act"), India's primary antitrust legislation. These actions were challenged by both Amazon and Flipkart in courts, but these challenges were struck down. It remains to be seen what the findings of the CCI's investigation are, and whether any penalties or corrective actions are imposed upon these e-commerce platforms.

The space of mobile OS and app ecosystems has also seen scrutiny from antitrust regulators. As an illustration, the CCI in 2022 passed an order imposing substantial fines on Google. In its order, the CCI found that Google's practices regarding the Android OS and the Android app ecosystem amounted to a violation of the Competition Act. The mandatory installation of the Google suite of apps (including Gmail, Google Maps, etc) and the denial of access to competing web search service providers, among other things, were held to be violative of the Competition Act by the CCI. Additionally, in a separate order, the CCI held Google's practice of mandating that app developers use Google's billing system to carry out in-app purchases also violates the Competition Act.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

No specific laws regulate cloud or edge computing in India. No specific regulatory licences need to be obtained from service providers. As with the response in **1. Metaverse**, a similar range of broad laws will be applicable.

Privacy

The SPDI rules will apply to the parties. Wherever sensitive personal data is being processed, this may only be done with consent that is obtained at the front end by the data controller (this is a practical observation, as no distinction between a data processor and data controller exists in the SPDI Rules). Under the DPDPA, such processing may only be justified as a result of consent obtained from the data subject, or through a reliance on a narrow band of other legitimate purposes. It is important to note here that the SPDI rules prescribe that the processor needs to have the same level of data protection standards as the party transferring the data to it. Under the DPDPA, there are no obvious restrictions on

cross-border data transfers, save the fact that the central government may notify a list of countries to which such transfers shall be restricted.

CERT-In Rules

On 28 April 2022, the Indian government notified a requirement for all service providers, intermediaries, data centres, body corporates and the government itself to report all cybersecurity incidents to the Indian Computer Emergency Response Team (the "CERT-In") within six hours of these incidents being noticed. Such cybersecurity incidents include a wide variety of occurrences, such as the unauthorised access of IT systems, identity theft, data breaches and data leaks.

Intermediary Guidelines

As is the case in the response to **1. Metaverse**, cloud service providers may well fall within the purview of an "Intermediary" as has been defined under Indian law. It is, however, important to note that in order to be able to successfully claim intermediary safe harbour, the other compliance obligations that are placed on the intermediary by way of statutes like the Intermediary Guidelines should be met.

Interception, Monitoring and Blocking

The Indian government, and in some instances, certain state governments, have powers to demand access to information, decryption and monitoring of information – for the purposes of public order, crime prevention/investigation and in the interest of national security. A failure to abide by a valid direction may lead to imprisonment and a fine. The Indian government may also issue blocking orders under similar provisions included within the IT Act and through subordinate legislation called the Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

India's banking regulator, the Reserve Bank of India (RBI), imposes a number of obligations on Indian banks. When it comes to storage of payment information, on 6 April 2018, the RBI issued a direction to all banks and Payment System Operators to store all payment data in systems located in India only, except in the case of cross-border transactions where a copy of the payment data, including the domestic component, may also be stored abroad.

Additionally, the Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, require that all insurers are to maintain records of their issued policies and claims, and these records, whether maintained electronically or otherwise, are to be maintained in India only.

The following aspects, in the context of the Indian legal landscape, may present challenges to the utilisation and functioning of cloud and edge computing services.

Breach notification

As stated above, cybersecurity incidents are to be reported to CERT-In within six hours of becoming aware of the incident, and a contravention of this directive carries with it penal provisions – imprisonment of up to one year, a fine of up to INR10,000,000 (approximately USD120,000), or both. Even though CERT-In has clarified that penalties for contravention will only be imposed in extraordinary cases for wilful non-compliance, practically speaking, this has led to a lot of friction between cloud service providers and their customers, which consist of corporations providing services to Indian customers and processing their personal informa-

tion, and has greatly complicated the negotiation of any such agreements. This issue is exacerbated by the fact that the global standard for data breach notifications (including as set out in the General Data Protection Regulation) requires data breaches to be reported within 72 hours of becoming aware of the breach.

Jurisdiction

As is the case with all internet-enabled technologies, the question of jurisdiction also poses a challenge in contravention by cloud and edge computing services. Even though the IT Act has been granted extraterritorial jurisdiction, actual enforcement against foreign entities who have no tangible presence in India is highly unlikely, and such entities may simply claim that the IT Act has no jurisdiction over them and refuse to comply with any requirements provided under the IT Act or rules framed thereunder while dealing with Indian consumers or business entities.

Cross-border data transfers

The Indian government may choose to restrict or block data transfers to countries which it feels are a threat to its national security. The DPDPA also has a specific provision which allows the Indian government to notify countries to which data transfers may be blocked. In 2022, the Indian government banned over a hundred apps with Chinese links, including major global players such as TikTok. This also presents a potential challenge to foreign cloud computing services operating in India, as a chance of being restricted or banned by the Indian government exists. As may be expected, the degree of this risk is contingent on India's geopolitical stances.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

There is no single Indian law that governs the use of AI in the country. A host of more general statutes, such as the IT Act, privacy law (currently through the SPDI Rules and in the near future, the DPDPA), and copyright law would be relevant in this space. Some of the things that stand out when considering laws that would govern AI apps, particularly those relevant for AI-generated content (AIGC) applications, are the following.

Web Scraping

The potential access to computer resources without permission of the owner has the potential to fall foul of various provisions of the IT Act. The scraping of information through automated means from websites that prohibit this under their terms of service may well also be considered a violation of contract. Clickwrap agreements have been held to be enforceable if they meet the other requirements of the Indian Contract Act, 1872, and a breach would open the door to remedies available under the law. Additionally, scraping may entail storing of copyright-protected works and their reproduction, which may give rise to claims of infringement. Each such scenario will need to be considered based on possible defences available under the law.

Intermediary Guidelines

It is possible, dependent on the use of AI made in each instance, that a platform may be considered to be an intermediary. In order to qualify thus, it would need to meet the test laid down in Section 79 of the IT Act – namely, that it does not initiate a transmission, select a receiver or exercise any editorial control. In the instance of AIGC specifically, it is unlikely that the third of these

tests would be met. Additionally, even if this test is met, the intermediary claiming safe harbour shall be required to comply with the obligations placed upon it by way of the law, including specifically under the Intermediary Guidelines.

Free Speech

Any content-generation AI will be subject to laws applicable to conventional forms of media, such as those prohibiting the hurting of religious sentiment, sedition and defamation.

Privacy

Even after being recognised as a fundamental right, the right to privacy is only guaranteed against the state, whereas its enforcement against private entities is dependent on statutes passed by parliament (such as the DPDPA) or subordinate legislation (such as the SPDI Rules). While the SPDI Rules continue to be applicable until rules that bring the DPDPA into effect are in force, the following considerations need to be borne in mind:

- the processing of any sensitive personal data will need specific consent; and
- data subjects will need to be provided the right to withdraw from further processing, as well as the right to correct their information.

The following points are of particular note under the DPDPA:

- consent, or other legitimate justifications permitted under the DPDPA, shall be required in each instance where personal data is processed (and not merely for sensitive personal data) as under the SPDI Rules;
- the definition of personal data under the DPDPA expressly excludes publicly available information;
- personal data of a data subject that has withdrawn consent is required to be erased unless reasonably required under any law;
- there are specific provisions under the law with regard to the processing of a minor's data which include the prohibition of behavioural monitoring; and
- there are other specific provisions that would be applicable to any AI app provider in the event it meets the threshold to be classified as a Significant Data Fiduciary – the threshold for which is yet to be notified. These shall include the need to carry out a data protection impact assessment, data audits, and the appointment of a Data Protection Officer.

Reports/Advisories/Best Practices and Guides

In 2018, the Ministry of Electronics and Information Technology, Government of India (MeitY), formulated multiple committees to work on different areas on AI to promote technology and develop a policy framework. These committees submitted multiple reports, including one on the Cyber Security, Safety, Legal and Ethical Issues associated with AI (the "MeitY Report"). It covers the new opportunities and challenges AI presents in the field of cybersecurity, including its potential use in combating cyberwarfare, the safety and privacy implications associated with such use of AI in the cybersecurity field, and the weaponisation of AI.

The MeitY Report also prescribes a comprehensive set of guidelines for the establishment of an accountability framework regarding AI technology.

In addition to the above, the apex public-sector think tank, NITI Aayog, in 2018 published a strategy document titled the National Strategy for Artificial Intelligence (the "NITI Report"),

based on the premise that India is in a position to emerge as one of the world's leaders in the AI space, focusing on the principles India can adopt to achieve social and inclusive growth "in line with the development philosophy of the government".

The NITI Report covers five major topics – global developments in AI, AI and India, focus areas for AI intervention, key challenges to AI adoption in India, and the way forward to harness AI (including research, re-skilling, accelerating adoption, and ethics, privacy, and security concerns).

It is important to note that neither the MeitY Report, nor NITI Report are in any manner legally binding.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There are no bespoke Indian laws that govern machine-to-machine (M2M) communication or IoT. The more general laws on privacy, interception, monitoring, blocking and breach reporting requirements would continue to apply.

It is important to point out here that there will be additional requirements that will be brought forth by the soon to come into force DPDPA, which would include a parallel data breach reporting requirement as well as greatly enhanced penalties for failures to ensure compliance.

Other than the above, the following may be of particular note.

- The government of India, in December 2016, approved 13-digit numbers for the purposes of M2M communication. Pursuant to this, allocations of 13-digit numbers to telecom service providers was carried out in 2018.
- In 2018, the Indian government issued a directive that issuers of SIM cards to be utilised for the purposes of M2M communications were to follow verification norms prescribed under the unified licence regime for telecom operators (as discussed in **7. Telecommunications**). The directive also prescribed a number of restrictive features to be implemented on such SIMs for M2M communication. The restrictive features were relaxed somewhat in 2019 further to representations by industry.
- In January 2022, the government issued a directive stating that a no objection certificate (NOC) would need to be issued by the Department of Telecommunication (DoT) for the sale or rent of International Roaming SIMs/global calling cards of foreign operators – including for the purpose of M2M communications. Only companies registered under the Indian Companies Act may make applications for the NOC, and in case of companies with foreign investment, they must be compliant with the extant foreign direct investment regulations of India. The directive also stated that where innovative app-based solutions were to be offered through the use of such SIMS, they would be approved by the DoT on a case-to-case basis pursuant to presentations and other requested information being submitted. NOCs are valid for a period of three years, with further renewal for up to three years at a time.
- In 2022, the government of India issued guidelines for the grant of a unified licence (as discussed in **7. Telecommunications**) which included authorisation for three categories of M2M services. Additional guidelines were also issued by the DoT in 2022 which inter

alia required the registration of M2M service providers.

In addition to the above, on 24 December 2023, the Indian Parliament passed the Telecommunications Act 2023 (the "Telecom Act"), which is aimed to replace the archaic Telegraph Act, 1885 (the "Telegraph Act") and the Wireless Telegraphy Act, 1933 (the "Wireless Telegraphy Act"). The new law will also be applicable to the M2M space, and will require holders of existing licences, registrations and permissions to eventually seek authorisation from the government. Provisions of the Telecom Act have been discussed in more detail in **7. Telecommunications**.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Currently, a number of pieces of legislation govern the provision of audio-visual media services in India. However, this legislation was put in place prior to the advent of the internet as a medium for audio-visual media, and as such, most do not include internet-based services within their ambit.

The Cable Television Networks (Regulation) Act, 1995 (the "Cable Television Act") governs the operation of cable television networks in the country, defined specifically as systems which are designed to provide cable services for reception by multiple subscribers. This legislation is restricted to terrestrial broadcasting mediums and does not include satellite television within its scope. The Cable Television Act requires all entities intending to operate as a cable operator to register themselves with the relevant authority. All cable operators are required to comply with the prescribed programme code and advertisement code, and not broadcast any programmes or advertisements which contravene the requirements of the respective codes. The Cable Television Act also imposes certain other obligations on cable operators, such as the requirement to mandatorily broadcast "Doordarshan" channels (TV channels operated by the Indian government), maintain certain registers, and transmit certain programmes/channels as prescribed by the Indian government.

Applications for approval to function as a cable operator are to be accompanied by the prescribed fee. Only individuals who are citizens of India, or companies incorporated under the laws of India, are permitted to register as cable operators.

Satellite television saw widespread adoption in India since the Indian government permitted its utilisation in 2000. In 2022, The Guidelines for Uplinking and Downlinking of Television Channels (the "Television Channel Guidelines") in India were issued by the Indian government to update and consolidate the regulations regarding operation of TV channels over satellite television. Different fees are prescribed for uplinking and downlinking of TV channels from within and outside India. Permission forms for a TV channel are to be accompanied by a prescribed fee. Annual permission fees as prescribed by the Television Channel Guidelines are to be paid for uplinking/downlinking TV channels in India as well. Additionally, the Television Channel Guidelines prescribe minimum net worth requirements to carry out these activities. The Television Channel Guidelines have also made the programme and advertisement codes prescribed under the Cable Television Act applicable on the TV channels being broadcast using satellite television, with penal actions ranging from an advisory

being communicated to the entity to suspension or revocation of permission.

With regard to internet streaming of audio-visual media, no specific legislation has been instituted yet. No specific registration or approval is required to operate an Over-The-Top (OTT) platform in the country. However, the provisions of the IT Act and the subordinate legislation framed thereunder, specifically the Intermediary Guidelines are applicable on such OTT platforms, as they fall under the definition of "intermediary" prescribed in the IT Act.

The Intermediary Guidelines require all intermediaries (including social media intermediaries – which would include hosts of user generated audio-visual content such as YouTube and Instagram) to abide by certain due diligence provisions in order to be beneficiaries of the "safe harbour" protection granted by the IT Act.

Obligations imposed by the Intermediary Guidelines (as discussed earlier) include the publication of the terms of use and privacy policy of the platform on its website or mobile app and provide an annual notice of these to users as well, and the obligation to inform users annually that in case of non-compliance with the platform's terms of use or privacy policy, their right to use the platform may be restricted. Additionally, intermediaries are required to make "reasonable efforts" to ensure that content hosted on the platform is compliant with certain conditions, such as those regarding obscenity, infringing upon intellectual property rights, content being deceptive as to its origin or information, or content which threatens the unity, integrity, defence, security or sovereignty of India, among other conditions. Intermediaries are also required to put in place a grievance redressal mechanism through instituting a Grievance Officer, who is required to acknowledge any complaint within 24 hours of receipt and resolve it within 15 days of receipt.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Various legislation and policies govern the telecommunications space in India. These include the Telegraph Act, the Wireless Telegraphy Act, and the Telecom Regulatory Authority of India Act, 1997.

The DoT, a department set up under the Ministry of Communications, government of India, has been granted the power to issue telecom licences under the Telegraph Act and Wireless Telegraphy Act. Further to the National Telecom Policy 2012 issued by the Indian government, unified licences are now granted by the DoT covering multiple telecommunications services, including access services, internet services, and national and international long-distance services.

Only companies registered under the Indian Companies Act may apply for the grant of a unified licence. Minimum net worth and equity requirements have been prescribed to apply for a unified licence, along with requirements for an entry fee and a bank guarantee. The extant foreign direct investment (FDI) policy of India allows for up to 100% FDI into entities engaging in the telecommunications space, however, security clearance from the Ministry of Home Affairs, government of India, is required to be obtained prior to such investments.

Upon the grant of the licence, licensees are required to pay an annual licence fee for each service area and each authorised service, cal-

culated as a percentage of the Adjusted Gross Revenue of the company. Licences are issued for a term of 20 years and may be renewed for ten years at a time upon payment of a renewal fee.

In addition to the licence, the DoT conducts periodic auctions to provide telecom companies with access to the radio spectrums for operating telecom networks. This process is separate and independent from the licence acquisition process.

In 2023, the Indian legislature passed the Telecom Act to overhaul and replace the existing telecom regime in the country. Although the Telecom Act has been passed by the Indian legislature, it will come into force at a later date to be notified by the government. This is expected later in 2024.

The Telecom Act updates and streamlines the currently disparate regulations which pertain to entering and operating in the Indian telecom industry. It retains the requirement for obtaining a licence from the government to operate a telecom business and clarifies that licences obtained prior to its institution under the Telegraph Act or Wireless Telegraphy Act shall continue until their date of validity after which they may be migrated to the fresh authorisation. Specific details as to the requirements of the licence under the Telecom Act will be put in place by delegated legislation (referred to as "Rules"), which have not been published yet. The Telecom Act has also been granted extraterritorial jurisdiction, and its provisions will apply to contraventions outside India if the contravention involves telecom services, equipment, or networks located in India.

Assignment of spectrums under the Telecom Act shall be conducted through auctions (except for certain specific purposes as listed for which the assignment shall be done through an administrative process). Similar to the licensing requirements, the requirements for being eligible to receive a spectrum assignment will be prescribed by the Rules.

The Telecom Act also grants the government the power to issue Rules regarding the protection of users, including on topics such as obtaining user consent before sending certain classes of messages, the institution of "Do-not-disturb" registers, a mechanism for users to report contravention of these measures, and the requirement for authorised telecom service providers to put in place a grievance redressal mechanism.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Essentially, while it may be viewed as an oversimplification, a technology transfer agreement is a contract that enables the movement of data, know-how and intellectual property from one organisation to another. The considerations discussed herein are of note while engaging in technology transfer agreements in India.

Foreign Exchange Regulation

Previously under the FEMA (Current Account Transaction) Rules, 2000, remittances for technical collaboration above a particular threshold required government approval, however, through a series of moves aimed towards easing business, these rules were relaxed.

Foreign licensors should, however, be conscious of the fact that the Foreign Exchange Management (Guarantees) Regulations, 2000, framed under the Foreign Exchange Management Act,

1999, do not automatically permit an Indian licensee or its owners to provide a personal or corporate guarantee to a non-resident without seeking permission of the regulator – ie, the RBI. There will be serious hurdles in the enforcement of such a guarantee.

Taxation

The Indian government has recently increased the quantum of withholding tax payable on royalties and fees for technical services of foreign entities by Indian parties.

A withholding tax will be required to be deducted by an Indian licensee from a foreign licensor of intellectual property. Licensors/transferors are advised to specify obligations in this regard in any agreement, including appropriate tax certificates proving payment.

The prevailing tax rate on royalties and fees for technical services is 20% plus applicable surcharge, but foreign licensors of intellectual property would be best advised to take advantage of various double taxation avoidance arrangements (DTAAs) that India has with most other nations.

In order to take advantage of DTAAs, the licensor will require a Tax Residency Certificate from its home country, register with the web portal of the Indian Income Tax Department, and provide a declaration that it does not have a permanent establishment in India.

Applicable Law and Jurisdiction

Usually, a party in the stronger bargaining position would look to ensure that the laws of its home jurisdiction would be the governing laws of the contract. As far as technology transfer agreements are concerned, this would usually be the licensor that would have the upper hand. As a consequence, courts of the home jurisdiction of the licensor would also ordinarily be provided exclusive jurisdiction over adjudicating disputes arising from the licence agreement.

The above having been said, licensors could face challenges enforcing foreign judicial awards, as Indian courts recognise the enforceability of only some foreign courts. Parties should consider this aspect before determining foreign jurisdiction in any agreements which would potentially require enforcement actions by Indian courts. Additionally, licensors would be well advised to retain the power in the agreement to approach courts in the licensee's jurisdiction to seek injunctive relief, should the relationship between the parties sour.

Adjudicating disputes in Indian courts also carries several challenges, not least the significant backlog of cases in the Indian judicial systems. Resolving disputes in Indian courts may take five to ten years (and possibly even longer).

If parties intend to adjudicate disputes through arbitration, care must be taken to ensure that the arbitration is held in a country that is notified as a reciprocating territory by the Indian government and is a signatory to the New York or Geneva Convention.

Stamp Duty

This is often a stumbling block from the point of view of foreign entities. For an agreement to be entered as evidence before Indian courts of law, it is necessary that the requisite stamp duty under the Indian Stamp Act, 1899, needs to have been paid. Until such requisite duties have been paid, the agreement may not be validly enforced or placed in evidence before an Indian court, which would then be bound to impound such an agreement and insist that the parties

pay the applicable penalties. Licensors should be conscious to insist that such obligations are completed by the Indian party from the get-go, and that the licence agreement itself carries a specific obligation in this regard.

Competition

Often, technology transfers are riddled with restrictive covenants, as well as minimum pricing directions upon the licensee. Licensors would be best served seeking specific legal assistance from local counsel on antitrust issues, such as restrictions on owners of the licensees to ever engage in competing businesses in the future, or deal with other parties that may be seen as competitors of the licensor. Provisions in agreements that have the propensity to be violative of Indian antitrust laws may be held to be void.

Similarly, provisions within these agreements that are overly restrictive on the business activities of the licensee as well as the owners of such licensee may be seen as agreements in restraint of trade and, as a result, unenforceable.

Intellectual Property

Under Indian law, patent licences are only valid if made by written agreement. Such licence needs to be registered with the Controller of Patents by way of the submission of a prescribed form with requisite fee.

Similarly, copyright licences are required to be in writing and duly executed in accordance with applicable law. However, there is no express requirement in the law for such licences to be registered with the Copyright Office.

Confidentiality

Strong confidentiality provisions in an agreement where information is the most important asset are a must. Even prior to the execution of the actual agreement, discussions between the parties should be subject to an NDA. The licensor should make it a point to mark information that is not for outside eyes as confidential specifically, to remove all doubt from the mind of a licensee's representative. The confidentiality provisions within the agreement should specify the requirement for access control measures, as well as the technological measures that the parties should put in place. Agreements should also specify the period after the termination and/or expiry of the licence agreement pursuant to which the confidentiality obligations shall continue to be applicable.

Various provisions of law may classify the unauthorised sharing of confidential information as a "breach of trust", while the IT Act also provides remedies against breaches of confidentiality as they relate to electronic records.

Indemnity and Related Provisions

Complications with regard to seeking guarantees from owners of the licensee have already been highlighted above in the heading titled "Foreign Exchange Regulation".

In addition, foreign licensors should be cognisant of the fact that liquidated damages according to Indian law may not be permitted to be unreasonable, and may not be inserted with the intent of penalising the breaching party.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Regulation of trust services in India is limited to legislation governing electronic signatures. Electronic signatures, their issue, use and legal

validity are governed by the provisions of the IT Act and rules issued thereunder. The IT Act grants legal recognition to electronic records and allows for the authentication of electronic records by way of digital signatures or electronic authentication techniques, which are considered reliable and are specified in the provisions. Conditions for reliability include the signature/authentication data being linked to the signatory, being under control of the signatory at the time of affixing, and any alterations to the signature/authentication or to the information after it is signed/authenticated being detectable.

Certifying Authorities are defined as those persons/entities who have been granted licences to issue Digital Signature Certificates (DSC) to end users under the provisions of the IT Act. Eligibility requirements for obtaining this licence include prescribed minimum paid-up capital and net worth requirements, as well as an FDI cap of 49%. Applications for licences are to be accompanied with a fee and a bank guarantee of the prescribed amounts.

Licences are valid for a period of five years from date of issue and may be renewed upon applications for such renewal. Certain obligations regarding reliability, security procedures, publishing of information, etc, are also imposed on Certifying Authorities by the IT Act.

End users may apply to a licenced Certifying Authority for obtaining a DSC and pay the prescribed fees for obtaining a DSC with a validity of two years.

India has adopted a digital identity system called *Aadhar*, which was initially launched in 2009. The *Aadhar* ecosystem is administered by the Unique Identification Authority of India, a statutory body set up by the Indian government. *Aadhar* numbers are unique 12-digit identity numbers which may be obtained by Indian residents. The assignment of the *Aadhar* number is linked to biometric and demographic data. *Aadhar* numbers are a mandatory requirement for availing of many government-provided services, subsidies and benefits.

As part of a challenge raised in courts against the constitutionality of mandatorily requiring *Aadhar* numbers for statutory benefits, the Supreme Court of India, in Justice KS Puttaswamy v Union of India, held that the right to privacy is enshrined with the fundamental right to life and liberty granted by the Indian Constitution (as discussed above). Via this judgment, the Supreme Court also struck down the provisions of the *Aadhar* legislation which allowed private entities to use *Aadhar* authentication. Such authentication is now only permitted when it is made permissible by a law in force.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com