

# International Comparative Legal Guides



Practical cross-border insights into digital business law

## Digital Business **2022**

**Third Edition**

Contributing Editors:

**James Gill & Victor Timon**  
Lewis Silkin LLP

**ICLG.com**

# Expert Analysis Chapters

- 1** De-risking Digital Business Dreams  
James Gill, Lewis Silkin LLP
- 5** Modern Slavery: A “Wicked Problem” that Requires a Human Rights-Based Approach  
Anne O'Donoghue & Palwasha Nawabi, Immigration Solutions Lawyers

# Q&A Chapters

- |  |  |
|--|--|
| <p><b>16</b> Brazil<br/>Mattos Filho: Fabio Ferreira Kujawski, Lisa Worcman, Paulo Marcos Rodrigues Brancher &amp; Thiago Luís Sombra</p> <p><b>26</b> Cyprus<br/>E &amp; G Economides LLC: Xenia Kasapi &amp; George Economides</p> <p><b>34</b> France<br/>Armengaud Guerlain: Catherine Mateu</p> <p><b>45</b> Germany<br/>SKW Schwarz: Dr. Christoph Krück, Franziska Ladiges, Alexander Möller &amp; Heiko Wunderlich</p> <p><b>53</b> India<br/>G&amp;W Legal: Disha Mohanty, Arjun Khurana &amp; Meghna Arora</p> <p><b>62</b> Indonesia<br/>Bagus Enrico &amp; Partners: Enrico Iskandar, Debu Batara Lubis &amp; Alwin Widjianto Hartanto</p> <p><b>71</b> Ireland<br/>Lewis Silkin LLP: Victor Timon</p> <p><b>83</b> Italy<br/>Portolano Cavallo: Irene Picciano, Donata Cordone, Fabiana Bisceglia &amp; Eleonora Curreli</p> <p><b>93</b> Japan<br/>Anderson Mori &amp; Tomotsune: Ken Kawai &amp; Takashi Nakazaki</p> | <p><b>101</b> Korea<br/>D'LIGHT Law Group: Iris Hyejin Hwang &amp; Kyoung Min Pyo</p> <p><b>107</b> Saudi Arabia<br/>Hammad &amp; Al-Mehdar Law Firm: Suhaib Hammad</p> <p><b>114</b> Sweden<br/>Synch: Jim Runsten &amp; Norea Normelli</p> <p><b>120</b> Switzerland<br/>Walder Wyss Ltd: Jürg Schneider, Hugh Reeves, Emilia Rebetez &amp; Maria Gentile</p> <p><b>129</b> Taiwan<br/>Lee and Li, Attorneys-at-Law: Robin Chang &amp; Eddie Hsiung</p> <p><b>136</b> Thailand<br/>Kudun and Partners: Kongkoch Yongsavasdikul, Koraphot Jirachocksubsin &amp; Suchaya Tangsiri</p> <p><b>142</b> United Kingdom<br/>Burges Salmon LLP: Andrew Dunlop, Matthew Loader, Liz Smith &amp; Laura Craig</p> <p><b>152</b> USA<br/>Cozen O'Connor: Victor J. Castellucci</p> |
|--|--|

# India

G&W Legal



Disha Mohanty



Arjun Khurana



Meghna Arora

## 1 E-Commerce Regulations

**1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2B e-commerce.**

In India, there is a great degree of overlap in legislation governing e-commerce and non-e-commerce businesses, such as the requirements for setting up a business, employment laws, and legal metrology legislation.

The legislation applicable to B2B e-commerce that governs foreign investments and the setting up of a business in India by foreign entities and individuals is the prevailing Foreign Direct Investment Policy (FDI Policy) and the Foreign Exchange Management Act, 1999, with the accompanying Rules. The FDI Policy prescribes: the maximum ownership that a foreign individual or foreign entity can have in an Indian entity engaged in certain business activity; the nature of business entity which can be established; the quantum of investment to be made for setting up or acquiring a business; and various other conditions that an Indian entity with foreign investment should comply with.

100% foreign direct investment is permitted in companies engaged in cash and carry wholesale trading and B2B e-commerce businesses. Such investment can be made without prior approval of the Government of India. Cash and carry wholesale trading, including sales through B2B e-commerce, would mean sale of goods or merchandise to retail, industrial, commercial, institutional or other professional business users, as opposed to end-consumers or retail customers for personal consumption.

The following conditions apply to companies with foreign direct investment engaged in B2B e-commerce:

1. **Customers to whom goods can be sold:** Sales should be made to retail, industrial, commercial, institutional or other professional business users, namely:
  - i. entities holding the applicable tax registration;
  - ii. entities holding trade licences (i.e. a licence or registration certificate, or membership certificate, or registration under the Shops and Establishment Act issued by a Government Authority reflecting that the entity or person holding the licence or registration certificate or membership certificate is engaged in a business involving commercial activity);

- iii. entities holding a permit or licence for undertaking retail trade; or
- iv. institutions having a certificate of incorporation or registration as a society or registration as a public trust, for their self-consumption.

2. **Records to be maintained:** Companies engaged in B2B e-commerce should maintain a complete record of sales on a day-to-day basis, such as the details of customers, their legal status (whether it is a company, partnership firm, sole proprietorship, trust, or society), their registration, licence or permit numbers, and the value of sale.
3. **Sales to group companies:** Sales of goods to one's own group companies should not exceed 25% of the total turnover of the company engaged in wholesale trading.
4. **Other registration and licences:** All other registrations and licences under local laws, as may be applicable to other entities engaged in a similar business, should be obtained.

**1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register, as well as a summary of legal obligations specific to B2C e-commerce.**

Certain specific pieces of legislation applicable in the context of B2C e-commerce are as follows:

- **Foreign Direct Investment (FDI) Policy:** The FDI Policy categorises models of business into marketplace models (the provision of an information technology platform by an e-commerce entity on a digital and electronic network to act as a facilitator between buyers and sellers) and inventory-based models (where the inventory of goods and services is owned by the e-commerce entity itself and sold directly to consumers). FDI is allowed in marketplace models where the e-commerce entity only provides a platform for buyers and sellers. Such B2C e-commerce entities with foreign investment will have to comply with the following:
  - i. An entity providing e-commerce services should be registered as a company under the Companies Act, 2013 (or under the Companies Act, 1956).
  - ii. E-commerce entities are permitted to enter into transactions with sellers registered on their platform on a B2B basis.

- iii. E-commerce entities can provide support services to sellers in respect of warehousing, logistics, order fulfilment, call/customer service, payment collection and other services. Such services could be provided to vendors on the platform on an arm's length basis, and in a fair and non-discriminatory manner by the e-commerce entity or other entities in which the e-commerce marketplace entity has direct or indirect equity participation or common control.
  - iv. E-commerce entities should not exercise ownership or control over the inventory (i.e. goods purported to be sold). Such an ownership or control over the inventory will render the business an inventory-based model. Inventory of a vendor will be deemed to be controlled by an e-commerce entity if the e-commerce entity permits more than 25% of its sales to be affected by one vendor or its group companies.
  - v. An entity with equity participation or inventory controlled by an e-commerce entity or its group companies is not permitted to sell its products on a platform run by such e-commerce entity.
  - vi. The website/platform where goods/services are made available for sale electronically should clearly provide the name, address and other contact details of the seller.
  - vii. Payments may be facilitated by e-commerce entities in conformity with the applicable guidelines of the Reserve Bank of India (RBI).
  - viii. Any warranty/guarantee of goods and services sold should be the responsibility of the sellers.
  - ix. E-commerce entities cannot directly or indirectly influence the selling price of goods or services and shall maintain a level playing field in a fair and non-discriminatory manner.
  - x. E-commerce entities will not mandate any seller to sell any product exclusively on its platform.
  - xi. E-commerce entities will have to obtain a report from a statutory auditor by 30 September of every year for the preceding financial year confirming compliance with the e-commerce guidelines under the FDI Policy.
- **Consumer Protection Act, 2019 (CPA 2019) and the Consumer Protection (E-Commerce) Rules, 2020 (E-commerce Rules):** These pieces of legislation are applicable to all B2C e-commerce entities. The E-commerce Rules apply to both local and international e-commerce entities irrespective of where they are established. The E-commerce Rules govern, among other things, grievance redressal mechanisms, the requirement to appoint a nodal officer to ensure compliance with the provisions of CPA 2019 and the E-commerce Rules, the obligations and liabilities of the e-commerce entity, false representation/advertising, violation of intellectual property, and manipulation of prices.

## 2 Data Protection

### 2.1 How has the domestic law been developed in your jurisdiction in the last year?

India does not (yet) have a dedicated data protection legislation. The Information Technology Act, 2000 (IT Act), with its companion rules and regulations such as the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011, along with a host of other sectoral regulations, seek to cover issues involving sensitive personal data, electronic transactions, cybersecurity, cybercrimes, etc., which confer upon citizens some degree of data protection.

The Personal Data Protection Bill was initially introduced in 2019 and was the first ever proposed law in India devoted to data protection, coming hot on the heels of an Indian Supreme Court judgment that declared privacy a fundamental right. It had, however, received its fair share of criticism on issues ranging from protectionism to arbitrary exceptions for data collection by the Government and surveillance concerns. More recently, a Joint Parliamentary Committee tabled its report on what is now the Data Protection Bill, 2021 (DP Bill). One of its most significant revisions is the expansion in its scope, which now seeks to cover non-personal data as well; additionally, the DP Bill now comes with a proposed timeline for compliance. Other aspects have remained the same as contemplated by previous revisions to the draft law, for instance: the classification of personal data (personal/sensitive/critical); data localisation in specific contexts; foreign entities that handle personal data of individuals in India; and the categorisation of "significant data fiduciaries" (with additional compliance based on volume of data). There is notable criticism against the DP Bill already, the biggest being that it retains provisions exempting the Government and also gives it wider discretion for collecting both personal and non-personal data of citizens without consent. That said, the DP Bill is yet to become law.

A related development in February 2021 was the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines). These seek to regulate social media intermediaries, streaming platforms and online publishers of news and current affairs by imposing stringent due diligence and compliance requirements – such as identifying the "first originator" of information (for intermediaries primarily offering messaging services), and the appointment of a chief compliance officer along with a resident grievance officer in India. Once again, the new Intermediary Guidelines have also been rightly criticised for implications such as granting power to the Government to block online content using emergency orders.

### 2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

India has seen a surge in the digital markets sphere, be it e-commerce, increasing online payments in a traditionally cash-reliant society, or tech-based health and financial services start-ups. By their very nature, such businesses handle large amounts of user data, which could potentially include personal information such as medical history and financial details. With that comes the risk of data being misused (or used beyond mutually accepted terms), especially with private players in various industries vying for access to more and more data/analytics to give themselves an edge – be it for targeted advertising, insurance checks, etc., in addition to hackers geared toward straight-up fraud. Consequently, some of the biggest challenges faced by data-driven businesses include: proper storage and protection of such data; issues of data ownership, consent and sharing with third parties; effective management of digital identities; and cloud-based security risks. In fact, fintech is perhaps a disproportionately likelier target for cyberattacks compared to most other industries, with KYC data being a goldmine for hackers. In March 2021, reports suggested that the personal data of over 3.5 million users of a popular Indian payments app were put on sale on the dark web – though the company denied a leak. Privacy compliance, therefore, becomes a large overhead for companies in this space, sometimes prohibitively so for smaller business. On the other hand, even with the Government recently making a push with the National Digital Health Mission (NDHM – which carries its own privacy concerns in the absence of dedicated

data protection legislation), India's healthcare space remains highly fragmented, with everything from single-doctor clinics to nationwide corporate hospital chains jostling for space – all, understandably, with different levels of technological capacity. Lack of standardisation and a resultant non-portability of digital health records remain a major challenge for organisations.

### **2.3 What support are the Government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health?**

In recent years, the Government has promoted campaigns such as Digital India to improve internet connectivity and online ecosystems, though its efficacy and implementation outcomes are up for debate as significant portions of the country still lack basic digital infrastructure. At the same time, there has also been a marked increase in FDI into India in retail and digital health, for instance Walmart's acquisition of Indian online marketplace Flipkart, and Tencent's investment into Practo, an Indian app for medical consultations and booking appointments.

A large unbanked population has made fintech an especially high-growth segment in India, with periodic regulatory changes having recently created "Payments Banks" – organisations that cannot offer loans or credit cards, but can carry out other banking functions. Given their existing infrastructures, several fintech and telecom companies are now entering this space. Successive legislative changes of questionable efficacy, for instance demonetisation and the Goods and Services Tax regime, have also led to a concerted push toward cashless technologies and digital payments, which – given the reliance on cash among much of India – have received notable Government promotion. Mechanisms such as Unified Payments Interface (UPI) and e-KYC have been adopted, and the Government has even promoted a homegrown payments app called Bharat Interface for Money (BHIM). The RBI has also released guidelines for a regulatory sandbox to allow stakeholders – including regulators, innovators and financial service providers – to test out new products and services in a controlled "live" environment, with certain regulatory relaxations for the purpose of testing. The Government is also pushing for necessary infrastructure to support the growth of fintech start-ups in the country. For example, the Government announced its intention to support the development of a world-class fintech hub at the International Financial Services Centre (IFSC) in Ahmedabad.

The use of AI is increasingly gaining traction as well, with the Government trying to foster a regulatory environment for this. For instance, in January 2020, India's Niti Ayog (the Government's policy think tank) recommended a cloud computing framework running on AI, called "AIRAWAT" (AI Research, Analytics and Knowledge Assimilation platform). Under this programme, the Government aims to promote the use and growth potential of AI by tackling challenges such as: lack of access to computers; assisting in the R&D of new technologies; and facilitating the work of stakeholders including start-ups, students, organisations and independent researchers. The Government also launched the National Artificial Intelligence (AI) Portal as a one-stop platform for all advancements pertaining to AI in India, and partnered with the industry to help AI-based start-ups showcase their products as a part of its "Atmanibhar Bharat" or "Self-Reliant India" initiative.

Policies are also being formulated in the digital health space, with the Government's announcement of the NDHM in July 2020, aiming to create unique health IDs to hold digital health records – although its potential implementation in the absence of a specific data protection law also carries data abuse and

privacy risks. The National Health Authority (NHA) is slated to play a role in the development of these policies and in managing the NDHM as a Government regulator.

## **3 Cybersecurity Framework**

### **3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.**

The IT Act and the rules made under it is the umbrella legislation which defines and governs cybersecurity in India. It covers a wide range of topics within its fold, including granting legitimacy to digital operations by prescribing modes of electronic execution of documents, prescribing data protection measures, penalties for cybercrimes and security of electronic data, to name a few.

The Indian computer emergency response team is responsible for analysing and addressing instances of cyber incidents and disseminating information regarding best practices to be followed for preventing cyber incidents.

Among other issues, the IT Act prescribes that an online business dealing with processing sensitive data must implement reasonable security measures and procedures. This is applicable to both B2B and B2C businesses. Further, if there is collection of sensitive data, there must be consent of the consumer and information regarding how it is collected and used by the company.

Further, the Payment and Settlements System Act, 2007 is a specific law which regulates payment operations and payment intermediaries in the e-commerce space. The RBI also issues guidelines regarding use of payment instruments, which includes debit cards, credit cards, e-wallets or gift cards.

Additionally, the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 impose certain duties on e-commerce entities which are to be duly followed by them. These rules have created a distinction between obligations of e-commerce entities and sellers selling through the platform.

### **3.2 Please provide details of other cybersecurity legislation in your jurisdiction. If there is any, how is that enforced?**

In addition to the legislation listed in question 3.1, under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, reasonable security practices and procedures must be implemented by all companies that process, collect, store, analyse or transfer sensitive data or information. Specific security measures are to be implemented by companies that have protected systems as prescribed under the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018.

The Companies (Management and Administration) Rules, 2014 require that companies must ensure all electronic records and security systems are insulated from data tampering and unauthorised access. The Indian Penal Code, 1860 also deals with some offences that may take place online, such as obscenity, defamation or cheating.

The intermediaries are regulated through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (see question 2.1), which state that intermediaries must provide reasonable security practices and procedures as per the SPDI Rules to provide security to their data resources and information. The intermediaries are required to report all

cybersecurity incidents to the Indian Computer Emergency Response Team (CERT-in). Any instances of non-compliance can disentitle intermediaries from claiming safe harbour provisions under the IT Act.

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 are responsible for creating the CERT-in. It is an administrative body responsible for collecting and analysing information on cybersecurity incidents and accordingly responsible for responding in emergencies.

## 4 Cultural Norms

### 4.1 What are consumers' attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or does a more cash-friendly consumer attitude still prevail?

According to a 2018 study, over 120 million users were expected to shop online that year, while India's e-commerce industry is expected to reach USD 200 billion by 2026. Even so, conventional brick-and-mortar retail has always dominated the larger retail market, especially in more remote parts of the country that still lack a serviceable digital infrastructure.

In a large and diverse country like India, consumers' attitudes can understandably not be homogenous; they are necessarily affected by, and must be seen in the context of, a multitude of often intersectional issues such as geography, class and economic status, and access to infrastructure. The probability of the average consumer leaning toward e-commerce – and having access to the internet in the first place – will depend upon a combination of these factors. That said, with growing competition and developing technology leading to an increase in internet penetration and affordability, India's active internet user base has crossed 560 million, which, for context, is still less than half the population.

Although the digital payments market in India is projected to grow to USD 1 trillion by 2023, India has traditionally been a cash-reliant society for several reasons (see question 4.2 below). Other initial deterrents for consumers have included the fear of disclosing financial data (through online payments) and the inability to try or test the look and feel of a product prior to purchase. Therefore, e-commerce companies have had to innovate aggressively and tailor their business models to suit local needs and compete with the ubiquitous mom-and-pop or *kirana* stores by offering multiple payment options such as cash-on-delivery (CoD) and monthly instalments, adopting liberal exchange/return policies and the like.

Most recently, the COVID-19 pandemic has also played a major role in shifting consumers' attitudes toward e-commerce, among those who can access and afford it. With strict lockdowns making it impossible (and sometimes illegal) to visit physical stores, consumers increasingly embraced e-commerce for its convenience.

### 4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery-type culture?

India has historically been cash-reliant for a variety of reasons, such as: a large unbanked population; a perceived mistrust of, and lack of access to, formal banking systems (and later online payments); tax evasion; and the dependence of small and medium business ecosystems, as well as households, on cash

transactions. In the context of e-commerce, studies show that a disproportionate majority of Indians prefer cash-on-delivery (CoD) while shopping online, which all major e-commerce players have had to factor into their strategies. CoD options bring their own logistical challenges, and it is not uncommon for e-tailers to provide additional discounts if buyers opt for digital payments, to promote the latter. Since credit card usage in India is negligible outside urban/metropolitan areas – estimates put it at about 3% of the population – digital payments have also adapted to the Indian landscape, with options including digital wallets such as Paytm and PhonePe and online payment systems such as Google Pay becoming increasingly prevalent.

### 4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Indian retailers and e-commerce platforms undoubtedly perform well within their own jurisdiction with Indian consumers. Unicorns like Flipkart, Paytm, Zomato and OYO Rooms have maintained commanding positions in their respective markets due to their perceived insight and understanding of the target audience, although this is not absolute and is affected by industry-specific peculiarities like anything else. In the food-tech space for instance, homegrown Zomato and Swiggy have outperformed UberEats; Paytm leads in the digital payments space, but Google Pay is not insignificant either; among online retailers, Amazon is second only to Flipkart. Practically however, most major Indian platforms increasingly have significant foreign investment – Flipkart is now owned by Walmart, while One97 Communications (Paytm) has raised funding from ANT Financial, SoftBank and Berkshire Hathaway, among others. Interestingly, however, as is the case with both Flipkart and Paytm, these platforms/companies are considered "Indian" as long as they have Indian founders, regardless of current funding or controlling interest.

As of now, no domestic platform/website occupies a dominant position in any international market. Of the Indian unicorns, OYO Rooms (whose investors include SoftBank and Airbnb) is perhaps one of the few to have seen rapid expansion outside India, though its success is debatable. While e-commerce in India has boomed in recent years, online retail still constitutes only a small percentage of India's total retail market – so it is perhaps good business for Indian platforms to first consolidate domestically, in a high-potential Indian market, before expanding into already saturated foreign jurisdictions. The Government has also been pushing for initiatives such as "Make in India" and is continuously doubling down on nationalistic sentiments by encouraging the public to use and support domestic, locally made/offered products and services.

That said, considering the exponential rise India has seen in the number of mobile (and internet) users over the past few years, there seems to be scope for the growth of e-commerce exports in the future.

### 4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Hindi (including its various dialects) is the most widely spoken language in India, with English a distant second, and most e-commerce firms will tend to switch between at least those two for the most part – Amazon's Alexa and Google Assistant

“understand” both Hindi and English. That said, India’s size and diversity brings with it a multitude of different cultures, regional identities and languages, which e-commerce firms, like any other business, must cater to. It is not uncommon for multinationals to advertise festive season sales and create brand campaigns in several Indian languages (along with Indianised/vernacularised English) simultaneously, while local counterparts like Flipkart, Snapdeal and Jabong have been multilingual for some time now. However, since Indian e-commerce firms are yet to make a meaningful expansion abroad, their handling of language barriers is yet to be tested.

#### **4.5 Are there any particular web-interface design concepts that impact on consumers’ interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.**

India is a highly complex jurisdiction, where significant inequities in opportunities and outcomes mean that a one-size-fits-all approach can never work. For instance, in spite of smartphone penetration and internet use, a significant section of the population still struggles with literacy. Therefore, platforms with a more visual style of interaction have historically seen more users than those that rely more on a text-based interface. This has also led to companies increasingly tailoring their UI/UX to suit local needs and sensibilities, by eschewing more complicated interfaces in favour of cleaner/simpler ones, such as tap-and-pay/one-touch payments in the digital payments space.

Additionally, a significant majority of Indian internet users access the internet primarily on mobile devices. This bit of local context means that, depending on the target consumer base, interfaces that are more mobile-friendly or “mobile first” tend to perform better than those optimised for computers; similarly, lighter interfaces/apps that consume lesser mobile data may be preferred by certain sections of consumers.

#### **4.6 Has the COVID-19 pandemic had any lasting impact on these cultural norms?**

The pandemic has decidedly had an impact on these norms, albeit among certain consumer bases. Extended lockdowns have shaped consumer behaviours *vis-à-vis* digital payments and using e-tailers for everyday needs such as groceries for instance, but only for consumers with access to that infrastructure. At the same time, it is not unusual to see elders going back to their corner store because of familiarity, or reverting to cash for comfort.

That said, the pandemic has certainly made consumers switch from physical retailers to e-tailers, some for the first time. The longevity of this trend, however, remains to be seen.

### **5 Brand Enforcement Online**

#### **5.1 What is the process for online brand enforcement in your jurisdiction?**

In India, there are a variety of ways whereby entities can undertake online brand enforcement, depending on the nature of the infringement/violation itself. For instance, finding counterfeits or products under confusing similar brands on online marketplaces is not uncommon, and most major e-tailers like Amazon and Flipkart have a dedicated internal reporting mechanism through which brands/rights owners can flag such listings and ask for their removal. In other cases, where infringements take

place on standalone websites or social media platforms, “take-down” notices are a fairly common and, in most cases, effective remedy sought by brand owners. For situations where a website/domain is itself in violation of a brand owner’s rights, proceedings against infringing domain names are possible under the .IN Domain Name Dispute Resolution Policy or INDRP, which is the UDRP equivalent for .IN domain names. These are apart from formal legal remedies available under the Indian Trademarks Act, 1999, as well as under common law – such as seeking injunctive relief and/or damages.

#### **5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?**

While there are no statutory restrictions *per se*, one of the biggest challenges that brand owners face is with cross-border enforcement. In situations involving brands that are unregistered and/or unused in India, establishing a trans-border/spill-over reputation in India becomes paramount, which is easier said than done when it comes to documentary evidence. That said, Indian jurisprudence on this issue has evolved over time; with businesses moving online and borders shrinking, Indian courts are increasingly giving online brand-use the evidentiary value it deserves.

With respect specifically to domain name issues, some domain registrars have begun masking/redacting information about domain owners in compliance with the GDPR, even when the domain owner is located outside the EU. This sometimes makes it difficult for a brand owner to ascertain information about the user/owner of an infringing domain name, in cases where formal proceedings under INDRP/UDRP are being contemplated. However, in the Indian context, there are practical workarounds to this that can be assessed on a case-by-case basis.

### **6 Data Centres and Cloud Location**

#### **6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?**

The Ministry of Electronics and Information Technology has issued certain Guidelines for Government Departments on Contractual Terms Related to Cloud Services. The Guidelines highlight key contractual terms that should be incorporated by Government Agencies in their contracts with cloud providers. The Guidelines also state that data provided by the Government Agencies to cloud service providers should be stored in India.

The IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 apply to insurers registered with the Insurance Regulatory Development Authority of India, with respect to any outsourcing arrangements they may enter into. These Regulations prescribe certain conditions with regard to obligations of service providers regarding confidentiality and security of information of policy holders.

Other than the above, there is no specific law in India on contracting with third party-owned data centres and cloud providers. However, the entities dealing with personal and sensitive information of natural persons should ensure that they are able to comply with the security standards and other conditions prescribed under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 with regard to collection, storage, processing, sharing and transfer of personal and sensitive information.

The relevant stakeholders should also keep a close watch on the new draft DP Bill, and if enacted may introduce additional

conditions relating to collection, storage and processing of personal and sensitive information. This may invariably have some impact on the arrangement with third party-owned data centres or cloud providers.

#### **6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?**

The need to localise data centres and servers is currently mandatory for certain financial and payment-related data. The RBI requires that all data collected by the payment system providers should be stored in a system in India.

Internet and telecommunication service providers are subject to the terms of the Unified Access License granted by the Government of India, which, among other things, requires that such service provider should not transfer (a) any accounting information relating to the subscriber, and (b) user information (except for international roaming/billing or information relating to foreign subscriber) to any person/place outside India.

Other than the abovementioned IRDAI Regulations, there are other sector-specific compliance obligations for location of servers/data centres. Additionally, refer to our response to question 6.1.

## **7 Trade and Customs**

#### **7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your jurisdiction?**

The Government of India in the last few years has taken several measures to digitise the cross-border trade process. Some of the key processes where the technologies have been adopted are:

- **The Indian Customs and Central Excise Electronic Commerce Gateway (ICEGATE)**, which is the national portal of the Central Board of Indirect Taxes and Customs and provides e-filing services to importers, exporters, cargo carriers and other trading partners electronically. ICEGATE can be used for filing bills of entry and shipping bills, and for electronic payment of customs duty.
- **The Portal for e-BRC Services**, which is an integrated platform which enables electronic transmission of Foreign Exchange Realisation Information from Banks directly to Directorate General of Foreign Trade's (DGFT) server. This portal also facilitates the issuance of electronic Bank Realisation Certificates by banks to the exporter for the purpose of claiming benefits under the various schemes of the Foreign Trade Policy.
- **The Export Data Processing and Monitoring System (EDPMS)**, which is an online platform for monitoring export returns.
- **The Import Data Processing and Monitoring System (IDPMS)**, which is an online platform for monitoring import returns.

Apart from the above, HSBC Bank, owing to the difficulties involved in cross-border trade and transactions, rolled out its new UniTransact platform, which aims to make cross-border transactions easier. The organisation Swift (a cooperative of banks globally that acts as an intermediary between these banks) is pushing for a standard and uniform digitisation of trade documents across banks, and has recently agreed with Axis Bank to test out the new environment for cross-border payments. Another private company, Piramal Glass, using blockchain technology, has successfully started their first cross-border trade digitisation programme.

#### **7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forward?**

One of the significant barriers to adoption of technologies is the reluctance of Government officials to use technologies more often to promote trade, resulting in red tape and demands for bribes. It will need constant efforts from all stakeholders to keep pushing the Government and its officials to promote the use of technology for trade facilitation.

## **8 Tax Treatment for Digital Businesses**

#### **8.1 Please give a brief description of any tax incentives of particular relevance to digital businesses in your jurisdiction. These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.**

Although the Government provides certain fiscal incentives to small businesses and start-ups in general, there is no specific tax incentive for digital business.

#### **8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?**

The Government of India has recently imposed an equalisation levy on the consideration receivable by an e-commerce operator not having permanent establishments in India in respect of transactions relating to online sale of goods and services in India. The levy is to be paid on consideration received by the e-commerce operators from persons resident in India, or a non-resident who buys goods or services, or both, uses an IP address located in India. After this matter received significant push back, the Government issued a clarification stating that offshore e-commerce platforms that sell their goods or services through their Indian arm will not be liable to pay such levy.

The Government also established a law to tax non-resident entities that do not have any establishments in India on the basis of "Significant Economic Presence" based on factors such as digital presence, number of users and revenue. It is likely that some of the overseas businesses engaged in digital business may come under the ambit of the new tax regime.

It is likely that these two areas may lead to a significant number of future cross-border disputes between digital business and Indian tax authorities.

## **9 Employment Law Implications for an Agile Workforce**

#### **9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please describe the advantages and disadvantages of the available employment status models.**

In India, various state- and centre-specific legislation governs employment. There are around 165 labour laws, around 50 of which are central pieces of legislation. Recently, the Government has amalgamated 44 central labour laws into four labour codes, which are yet to be notified.

This legislation includes workmen, skilled employees, unskilled employees, contract labourers, etc. Employment is usually executed through employment agreements which are governed by the Indian Contract Act, 1872. The employment agreements have to be in line with the applicable labour legislation. Terms of agreement which are in contravention of the labour legislation may carry a penalty under the relevant legislation.

The employment is governed through contractual terms and labour laws which provide certain rights to the employees through the Maternity Benefit Act, Employees' State Insurance Act, Employees Provident Fund Act, Payment of Gratuity Act, etc.; such labour legislation make binding obligations on the employer to provide benefits to his employees. The labour laws are a safeguard for employees that protect them from unfair contractual terms. The labour laws provide employees with benefits such as rights to leave, prevention of sexual harassment, appropriate working hours, bonus, etc.

India is heavily regulated in the employment sector. It is pertinent to seek legal assistance in the structuring and hiring of employees to avoid any penalties under the various legislation.

#### **9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation's physical premises?**

There are no specific regulations in India relating to carrying out work away from an organisation's physical premises. As such, the employee shall be governed by the employment agreement and the internal policies of the company. Also, the company has to fulfil its obligations toward the employees as required by the legislation governing employment.

There have been recent reports that the Government of India is looking to enact a detailed policy that will govern working from home (WFH) for employees across all sectors. The policy is reported to address concerns such as employers' liability toward their employees, number of working hours and basic expenses incurred by employees while WFH, such as electricity and internet costs.

#### **9.3 What long-term effects or changes are likely to result from the COVID-19 pandemic?**

The COVID-19 pandemic has brought about a paradigm shift in the work policies in many companies. Many companies are planning to implement hybrid work policy structures, blending WFH, working from any location and working from the office. It is likely for various other companies to follow suit.

Additionally, due to the pandemic, there has also been a shift from physical record keeping to digital record keeping, which is a trend we anticipate will continue even post-pandemic. Further, changes in meetings, including board meetings, will take place through video-conferencing. Indian legislation already has structures in place to implement such changes.

### **10 Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions**

#### **10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?**

Absence of well-defined laws (and ambiguity in existing regulations) is the key barrier for growth of digital business in India. Apart from that, general issues such as cybersecurity threats, availability of digital talent and associated costs are major

barriers – a fact also recognised in the latest edition of the DBS Digital Readiness survey – which also identified the high cost of incorporating the required technology as an impediment for smaller businesses.

#### **10.2 Are there any notable advantages for a digital business operating in your jurisdiction?**

With a population of 1.3 billion – significant portions of which are unbanked and may not be online yet – India provides enormous opportunities for the exponential growth of digital business. A sizeable and growing consumer base, along with existing and prospective legislative reforms, are a big positive for digital business in India.

#### **10.3 What are the key areas of focus by the regulator in your territory in respect of those operating digital business in your territory?**

The key areas of focus of regulators in India in the areas of digital business are: (i) the extent and conditions for foreign investments in e-commerce business in India; (ii) protection of small business enterprises engaged in retail business from abuse by dominant e-commerce entities; (iii) consumer protection; (iv) protection of personal and sensitive information of natural persons; and (v) taxation of e-commerce operators not having permanent establishments in India on the basis of their significant economic presence in India.

### **11 Online Payments**

#### **11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?**

In India, all regulations relating to payments and settlements are governed by regulations that set by the RBI. Significant regulations include:

- The Payment and Settlement Systems Act 2007 (PSSA), which regulates payment systems in India. The PSSA defines payment systems as systems that enable payments to be effected between a payer and a beneficiary, involving clearing, payment or settlement service, or all of these.
- Know Your Customer (KYC)/Anti-Money Laundering (AML)/Combatting Financing of Terrorism (CFT) Guidelines as issued by the RBI from time to time. These Guidelines are applicable to all payment aggregators and gateways under the PSSA.
- RBI (Digital Payment Security Controls) Directions 2020, for scheduled commercial banks (excluding regional rural banks), small finance banks, payments banks, and credit card issuing non-banking financial companies to set up governance structures for such systems and implement common minimum standards of security controls for channels like the internet, mobile banking and card payments, among others. The Guidelines create an enhanced and enabling environment for customers to use digital payment products in a more safe and secure manner.
- RBI (Guidelines on Regulation of Payment Aggregators and Payment Gateways) directs companies/payment aggregators to delete sensitive information related to their debit or credit cards from their servers and instead use "encrypted tokens" to facilitate transactions.

**11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?**

India has a comprehensive law to govern online payment service providers. A number of regulations and guidelines apply to service providers depending on the nature of services provided. The key challenges involve understanding the complex regulatory framework, some of which may not be entirely well defined.

## 12 Digital and the Green Economy

**12.1 With the current global emphasis on the environment and sustainability, is there any current or anticipated legislation in that area which is likely to impact digital business in your jurisdiction?**

There is, at least at the moment, no law already in place or anticipated legislation that could satisfactorily deal with the issue of sustainability and environmentally friendly practices in the digital space for businesses in India.

**12.2 Are there any incentives for digital businesses to become "greener"?**

There are no significant incentives provided by the Government for digital businesses to become "greener". That said, major companies (especially ones with a global presence) are on their way to adopting more sustainable practices on their own. There are several reasons behind this, from value building and wanting to retaining their customer base (seeing as consumers in the market are actively becoming more conscious about choosing brands that value sustainability and minimal environmental damage) to considering long-term cost-effectiveness.

**12.3 What do you see as the environmental and sustainability challenges facing digital businesses?**

Considering India is still a developing nation, one of the major reasons why digital businesses cannot properly adopt environmentally sustainable practices is due to the lack of resources and incentives. While switching to greener alternatives is easier for companies already at scale, for whom they may even be more cost-effective in the long run, the same is not true for a lot of the smaller players in the market. Another impediment is the lack of awareness – many businesses and investors are not aware of (and sometimes actively ignore) the magnitude of the environmental impact their businesses can have, although this is slowly changing for the better. As corporate social responsibility increasingly plays a role not just as necessary compliance but even as a selling point for companies – for instance, mobile-first foodtech and delivery start-ups focusing on organic products – sustainability should move on from being a buzzword to a legitimate organisational goal.

At the same time, the Government seems to be incentivising digital businesses; they may be viewed as more environmentally sustainable than traditional models of business in some sectors – although this not always true, and the environmental impact of technology is its own debate. Therefore, the focus seems to be to make digital business more prevalent in the market. It is likely that concerns about their environmental impact would catch the law-makers' attention after digital businesses take up more market share in the country.



**Disha Mohanty** is a Principal at G&W Legal. She chairs the firm's Corporate/Commercial practice, and co-heads the Digital Business industry group.

Disha has extensive experience advising clients on a broad spectrum of matters, including commercial contracts, franchise and distribution, regulatory compliance, foreign investment, employment law and real estate. She works with clients across multiple sectors ranging from retail and e-commerce, F&B, tech, pharma, consumer electronics, etc. Representatively, Disha assists a multinational apparel company with all aspects of setting up and scaling its operations in India, counsels a global semiconductor company, and helps a large Australian retail chain with employment law and other matters concerning its Indian operations.

**G&W Legal**

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

Tel: +91 9958 3485 59

Email: dishamohanty@gnwlegal.com

URL: www.gnwlegal.com



**Arjun Khurana** is a Principal at G&W Legal. He chairs the firm's Technology, IP and Media practice and co-heads the Digital Business industry group.

Arjun's practice traverses Privacy and Data Protection; Technology and Emerging Issues; Advertising & Marketing; IP; and Digital Ventures. He currently sits on INTA's Data Protection Committee and is a member the International Association of Privacy Professionals. Arjun advises Fortune 500 companies as well as SMEs at the intersection of emerging tech and the law; guides clients through the changing data protection and privacy regime in India; acts on complex cross-border IP and technology transactions; and represents clients in commercial disputes. He has significant experience helping international businesses navigate the Indian legal landscape. Notably, Arjun represents one of the world's largest media networks in high-value litigation; advises an internet giant in connection with its AdTech business in India; counsels a global tech and consulting powerhouse on all aspects of its digital ventures vertical in India; and advises the most valuable global sportswear brand on its Indian franchise and retail operations.

**G&W Legal**

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

Tel: +91 8800 1165 14

Email: arjun@gnwlegal.com

URL: www.gnwlegal.com



**Meghna Arora** is an Associate at G&W Legal. She is part of the firm's Technology, IP and Media practice, and has an interest in data protection and privacy issues.

**G&W Legal**

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

Tel: +91 1161 3483 06

Email: meghnaarora@gnwlegal.com

URL: www.gnwlegal.com

Combining the experience of big law firms with the expertise of a boutique, G&W Legal is a full-service business law firm that assists its clients at the intersection of law and pragmatism. Our team spans diverse subject matters and industries, using its robust skillset to become greater than the sum of its parts.

As the world grows smaller in the information age, business is no longer limited by borders. We understand this well, and provide our clients with advice and representation on every aspect of expanding into and doing business in India. Our attorneys bring a rich body of knowledge and accomplishment across (often intersecting) areas such as: Corporate/Commercial; Intellectual Property, Tech and Media; Franchising and Distribution; Advertising and Marketing; Privacy and Data Protection; Product Liability and Consumer Protection; International Trade; Foreign Investment; Private

Equity and Venture Capital; Employment; Government Contracts; Corporate Restructuring; Corporate Governance, Ethics, Compliance and Investigations; Anti-trust/Competition; Regulatory Affairs; Real Estate; Dispute Resolution; and everything in between.

[www.gnwlegal.com](http://www.gnwlegal.com)

G&W

Legal

# ICLG.com



## Current titles in the ICLG series

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Finance & Leasing
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Consumer Protection
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Tax
- Cybersecurity
- Data Protection
- Derivatives
- Designs
- Digital Business
- Digital Health
- Drug & Medical Device Litigation
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Environmental, Social & Governance Law
- Family Law
- Fintech
- Foreign Direct Investment Regimes
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Renewable Energy
- Restructuring & Insolvency
- Sanctions
- Securitisation
- Shipping Law
- Technology Sourcing
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms