April 2022

THE TECHNOLOGY NEWSLETTER

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

INTRODUCTION

The Argus Technology Newsletter discusses recent developments in technological advances or milestones or events. As lawyers, we enjoy delving into the legal nuances and implications of technological changes and analysing their impact on our clients and their activities. It is said that law always lags behind technological advances and there could be some truth behind such statement, but there is no reason for lawyers to lag behind technological advances.

The Argus Technology Newsletter is not meant to be a substitute for your regular technology periodical. Instead, we hope and promise to offer a lawyer's insights into technological change and innovation.

Argus Partners has a developed a strong and a robust technology and data privacy practice, which spans transactional advisory, corporate and regulatory advisory as well as contentious matters and disputes. Whilst physically the attorneys are based out of our Mumbai, Delhi & Bangalore offices, the team is servicing clients across the globe on Indian legal issues in technology and data privacy.

SEBI Enters into the Web 3.0 – Security and Covenant Monitoring Using Distributed Ledger Technology

Article Contributed by Aryan Mohindroo (Associate)

The Securities and Exchange Board of India, on March 29, 2022, by way of the circular titled *Operational guidelines for 'Security and Covenant Monitoring' using Distributed Ledger Technology (DLT)* ("**Circular**") has issued operational guidelines for distributed ledger technology, as used in blockchains, to monitor compliance of security and covenants in relation to issuance of non-convertible securities.

The move follows the broad framework shared by the SEBI in August, 2021 by way of its Circular numbered SEBI/HO/MIRSD/MIRSD_CRADT/CIR/P/2021/618 dated August 13, 2021 which specified the manner of recording of charges and monitoring by intermediaries like Debenture Trustees and Credit Rating Agencies ("**CRA**"). The Circular spells out the working of the DLT system.

The Circular provides that each asset provided by the Issuer as a security shall be recorded on the DLT system and shall be allotted a unique 'Asset ID' which may be used for data exchange and verification across depositories. The Asset ID shall be a 12 digit alphanumeric string which will be a combination of various codes as spelled herein –

"Asset ID = System Code + Asset Type + Asset Sub Type + Unique Number + Check Digit"

To ensure that the uniqueness of an Asset ID is maintained and there are no duplicate entries, there will be appropriate validation and duplicate checks in the DLT system as well as alerts for Issuer and the Debenture Trustee wherein Issuer shall ensure that each entry made for an asset is unique, and the Debenture Trustee shall be entitled to verify the entries. Since the system is at a nascent stage, only limited assets will be tracked at the portfolio level, namely, the movable assets like furniture, equipment, inventory etc., the current assets, like advances and receivables and any other assets of similar nature.

On a yearly basis, the Debenture Trustees shall reconcile a list of assets recorded on the system for each issuer and shall take necessary steps to reconcile any incorrect/duplicate entries, if so found, verify the security cover for the same and take remedial measures for the

same if needed. Reduction of security cover below the legally mandated limits shall be updated by the Issuer. Termed a trigger event, the depositories shall send alerts to concerned stakeholders in case of trigger events.

Certain amendments have also been made to the August, 2021 circular including obligations of CRA towards uploading all credit rating information, rating action, date of press release and hyperlink for the press release of credit rating. Discrepancies, if any, may be notified by the Issuer and the CRAs on the system and update the information within 3 (three) working days of notification. The DLT system is applicable to issuances of non-convertible securities from April 1, 2022 and all Issuers shall be required to enter the details into the DLT system on or before September 30, 2022 and Debenture Trustees shall verify the said information by November 30, 2022.

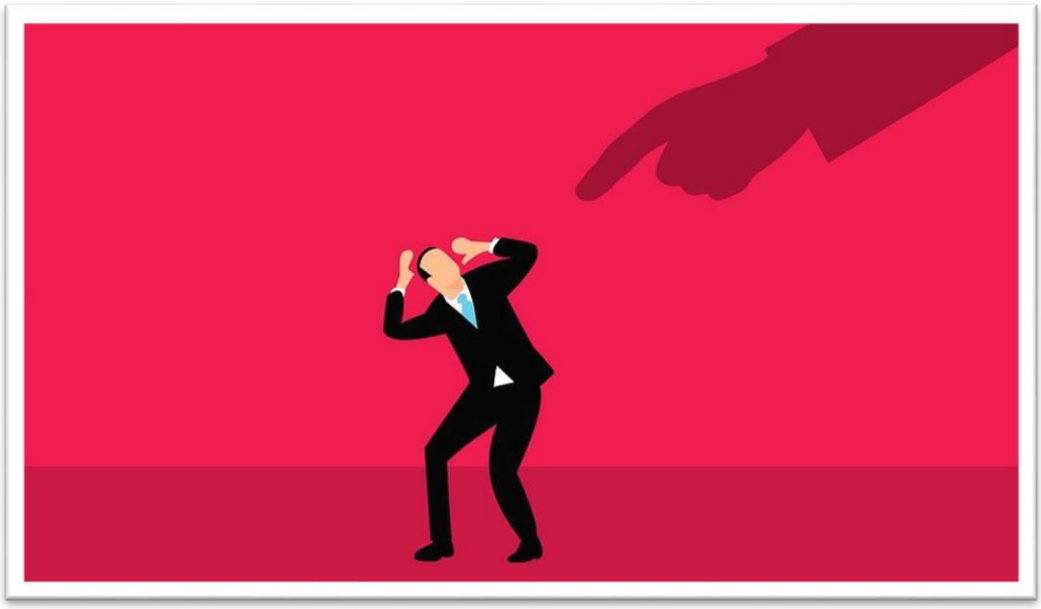
Argus Remarks

Even though the DLT is at a nascent stage and only involves a limited record of information, SEBI's move is a step in the right direction as the move will increase investor confidence and ensure constant monitoring of assets with a strong and unalterable transaction history.

Several issues still remain, but may be addressed in due course of time, including the ability to track an underlying security when the DLT has various NCD issuances running simultaneously and the regular monitoring and updating effort required throughout the life-cycle of the listed security.

Infosys Non-compete Clause: Whether it Amounts to 'Restraint of Trade'?

Article Contributed by Smriti Tripathi (Associate)



Infosys, one of the top 5 Indian IT firms, has imposed a negative covenant on all its employees. In its offer letter for new employees, Infosys has added the following non-compete clause: "*In consideration of the above, I agree that for a period of six (6) months following the termination of my employment with Infosys for any reason, I will not: (a) accept any offer of employment from any Customer, where I had worked in a professional capacity with that Customer in the twelve (12) months immediately preceding the termination of my employment with Infosys; (b) accept any offer of employment from a Named Competitor of Infosys, if my employment with such Named Competitor would involve me having to work with a Customer with whom I had worked in the twelve (12) months immediately preceding the termination of my employment with Infosys*." The 'Named Competitors' include TCS, IBM, Cognizant, Wipro and Accenture.

Hence, in case any Infosys employee who is has agreed to be bound by the new non-compete clause resigns, then for the next 6 months, that employee would be banned from working for TCS, IBM, Cognizant, Wipro and Accenture, in case they have the same clients as that of the Infosys employees in the last 12 months.

The entire IT industry is currently experiencing severe attrition and more than 80,000 Infosys employees have resigned in the last 3 months. If Infosys's employees cannot join a competitor after leaving Infosys, the number of employees leaving Infosys will be greatly reduced.

After receiving complaints from Infosys employees, Nascent Information Technology Employees Senate ("**NITES**") has filed a complaint with the Ministry of Labour & Employment. The Complaint states that "*The restriction contained in the employment letter is clearly in restraint of trade and therefore illegal under section 27 of the Contract Act. It is not seeking to enforce the negative covenant during the term of employment of the employee but after the termination of his service. The clause of covenant being imposed is to operate after the termination of services and is too widely worded, and hence the company should be stopped from enforcing it. The employee's covenants should be carefully scrutinized because there is inequality of bargaining power between the employer and employee, indeed no bargaining power may occur because the employee is presented with a standard form of employment*

contract to accept or reject. At the time of the employment agreement, the employee may have given little thought to the restriction because of his eagerness for a job. The contract of employment is likely to affect the employee's means or procuring a livelihood for himself and his family. The restraint being put on employees is greater than necessary to protect the employer, is unduly harsh and oppressive to the employee."

Section 27 of the Indian Contract Act, 1872 states that every agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind, is to that extent void.
There are two statutory exceptions to this rule – sale of goodwill and agreement between partners of a partnership firm. Apart from these statutory exceptions, the judiciary has devised various exceptions to this general rule, with reasonableness in scope, duration and geographical limit of the restrictive covenant being the touchstone for deciding whether the restrictive covenant amounts to a "restraint of trade".

One such judicial exception is restraint imposed by employers upon their employees. However, the judiciary while determining whether a negative covenant is in restraint of trade, business or employment or not, has taken a stricter view with regard to employer-employee contracts than in other contracts, such as collaboration contracts, franchise contracts or agency/distributorship contracts.

Negative covenants prohibiting the employee from working elsewhere during his term of employment in service agreements have been enforced by the Indian courts, maintaining that such restraint is reasonable to protect the interests of the employer as the employee is in possession of trade secrets, customer list etc. of the employer. In the case of ***V.N Deshpande* v*. Arvind Mills Co. Ltd***.[1], the court held that an agreement of service containing a negative covenant preventing an employee from working elsewhere during the term covered by the agreement was recognized in India. Court held that *the question whether a particular agreement was unreasonably wide had to be decided by the nature of the agreement, the qualifications of the employee, and the service he had to render along with the places where the employee could get alternative service of the same nature.*

However, the judiciary has refused to enforce post termination non-compete clauses in employment contracts as they have been held to constitute a "restraint of trade" under section 27 of the Act. Such agreements of restraint are held void because of being unfair and depriving an individual of his or her right to earn a living. In ***Brahmaputra Tea Co. Ltd.* v. *Scarth***[2], the condition under which the covenantee was partially restrained from competing after the term of his engagement with his former employer, was held to be void but the condition by which he bound himself during the term of his agreement, not to compete with his employer was held good. Courts have held that "*considerations against restrictive covenants are different in cases where the restriction is to apply during the period after the termination of the contract than those in cases where it is to operate during the period of the contract. Negative covenants operative during the period of the contract of employment when the employee is bound to serve his employer exclusively are generally not regarded as restraint of trade and therefore do not fall Under Section 27 of the Contract Act*."[3]

In light of the above, it can be seen that usually the courts do not uphold a restrictive covenant on an employee post termination of his employment but such a covenant could be upheld if it is proved to be reasonable to protect the interest of the employer. If we analyze the negative covenant sought to be imposed by Infosys on its employees, it can be seen that the prohibition

[1] 48 Bom. L.R. 90.
[2] I.L.R. (1885) 11 Cal 545.
[3] Niranjan Shankar Golikari v. The Century Spinning and Mfg. Co. Ltd. AIR 1967 SC 1098.

on the employee is limited to not working with certain Named Competitors of Infosys, *only if such employment would require the employee to work with a Customer with whom such employee had worked in the twelve (12) months immediately preceding the termination of his employment with Infosys*. Further, such a prohibition is only for a period of 6 months post termination of employment with Infosys. Given the nature of work in the IT industry and the real possibility of leak of confidential information of Infosys customers, this covenant could be deemed as reasonable if it is interpreted such that there is no blanket restriction on an employee from taking up work with a Named Competitor and such employee is allowed to work with any of the Named Competitors as long as it is ensured that the customers with which that particular employee works with are not the same as the customers with which the employee worked in the last 12 months of his employment with Infosys.

IAMAI Calls for a Risk-based Approach for Determining the Age of Consent under the New Data Protection Bill

Article Contributed by Anurag Prasad (Associate)

The Internet and Mobile Association of India ("**IAMAI**") which represents internet and tech-oriented companies and has executives from various tech behemoths such as Amazon and Microsoft on its governing council, has opposed the minimum age of 18 (eighteen) years required to give consent under the draft Data Protection Bill, 2021 ("**DP Bill**") contained in the report of the joint parliamentary committee ("**JPC**") published on December 16, 2021 ("**Report**").

While opposing a static and seemingly high age requirement of 18 (eighteen) years, IAMAI had proposed that a 'risk-based approach' should be followed by the Indian legislature and the regulators in determining the age of consent. A risk-based approach postulates that the age of consent should depend on the nature of the service being provided under a particular transaction involving an individual.

For instance, fixing the age of consent at 18 (eighteen) years to subscribe to a new financial services product such as a payment wallet makes sense. However, a child who is less than 18 years of age could be allowed to subscribe to an ed-tech platform at a much lower age.

IAMAI had also noted in its suggestions to the JPC that other countries have different ways of handling the age of consent debate. For instance, in the European Union, the age of consent is 16 (sixteen) years and for the United States of America, the Children's Online Privacy Protection Act fixes the age of consent at 13 years.

Over the last couple of years, this issue has been extensively debated upon, with many believing that India must align with global best practices. Any significant deviation would entail additional compliance requirements and added costs for global players.

Are 'Domain Name Registrars' Intermediaries under the Information Technology Act, 2000? – Delhi High Court Answers

Article Contributed by Niharika Sharma and Akshay Bhatia (Associates)

A Single Judge Bench of the Delhi High Court ("**Court**") recently held in the case of *Snapdeal Private Limited* v. *Godaddycom LLC & Ors.*, that 'Domain Name Registrars' are 'intermediaries' under Section 2(1)(w) of the Information Technology Act, 2000 ("**IT Act**").

Background facts

Snapdeal Private Limited ("**Snapdeal**") filed a suit seeking an omnibus injunction against Domain Name Registrars ("**DNRs**") from offering any domain names with its registered trademark - 'SNAPDEAL'. Snapdeal alleged that, by offering, for registration of domain names which include the thread 'SNAPDEAL', DNRs are facilitating infringement of its registered trademark and are therefore infringers under Section 28 and 29 of the Trade Marks Act, 1999. Snapdeal also sought a *quia timet* injunction barring aspiring registrants from registering a domain including the words/ thread 'SNAPDEAL'. To support its case, Snapdeal also submitted that DNRs are not 'intermediaries' under the IT Act and therefore do not enjoy the immunity from liability under Section 79 of the IT Act. Based on various rival contentions made by both Snapdeal and DNRs, the Court framed the following questions of law and facts:

a. **Are DNRs 'intermediaries' within the meaning of Section 2(1)(w) of the IT Act?**
b. **Are DNRs entitled to 'safe harbor' under Section 79 of the IT Act?**

a. Are DNRs 'intermediaries' within the meaning of Section 2(1)(w) of the IT Act?

The Court has answered this in affirmative.

Section 2(1)(w) of the IT Act defines 'intermediaries', which, '*with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places*

and cyber cafes'. For the words '*with respect to*', the Court observed that services '*with respect to*' electronic records would, include, within their scope and ambit, the service of providing electronic records, being domain names in this case, for utilization by aspiring registrants.

The Court after analyzing the definitions of 'electronic record', 'data' and 'information' held that the definitions of 'intermediaries'; 'electronic record'; 'data'; and, 'information' flow from one to the other, to qualify domain names as 'electronic records' as per Section 2(1)(t) of the IT Act, especially as domain names which are provided by the DNRs, are sourced from a common Domain Name Registry. As being persons who provide service with respect to domain names, the DNRs would be "intermediaries" within the meaning of Section 2(1)(w) of the IT Act.

The Court further observed that as the DNRs fall within the 'means' part of the definition of 'intermediaries', and therefore it was not necessary to examine the categories of intermediaries envisaged by the 'includes' part of the said definition. For this reliance was placed on the Supreme Court's decision in *Black Diamond Beverages Vs. Commercial Tax Officer (1998) 1 SCC 458*.

b. Are DNRs entitled to 'safe harbor' under Section 79 of the IT Act?

Having held that DNRs are intermediaries under the IT Act, the Court was faced with the question of whether such DNRs would be entitled to 'safe harbor' under Section 79 of the IT Act, to which the Court answered in the negative.

Section 79 of the IT Act provides for the exemption, from liability, of intermediaries in certain cases. Section 79(1) provides immunity to an intermediary from liability "*for any third-party information, data, or communication link made available or hosted by him*." Section 79(2) sets out conditions where the safe-harbor under Section 79(1) would apply, whereas Section 79(3) enumerates conditions where safe-harbor would not be applicable.

The Court held that in cases where an intermediary provides functions which are in excess of providing access to a communication system over which information made available by a third party are transmitted, stored or hosted, it cannot secure the benefit of Section 79(1). As is evident, DNRs in the present case are not merely providing access to a communication system over which information can be shared but are operating for profit, as a business enterprise. The Court stated that, the fact that such DNRs are providing alternative domain names for a price and are even differentially pricing the alternative domain names, depending on the demand for such alternatives, makes it clear that such an activity would traverse beyond the realm of Section 79(2)(a), which limits the scope of protection to intermediaries which are "*providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted*". Therefore, the Court held that safe-harbour under Section 79 of the IT Act would not be available to the DNRs if cases where it is found that any domain name provided by the DNRs infringes the registered trademark of any third party.

When intermediaries provide services which are outside the scope of the role of an intermediary, as defined under the IT Act, such as providing alternative domain names and brokerage services, the immunity provided under Section 79 of the IT Act would not be available to them with respect to such activities.

Even though this decision clarifies the position in relation to DNRs, it does not *stricto sensu* apply to traditional intermediaries, i.e., social media platforms such as Facebook and Twitter. This finding, even though given at a *prima facie* stage in the present case and limited to DNRs, would serve as an important marker to other intermediaries such as social media platforms,

internet service providers, search engines to understand the risks as well as the protection available to them under the IT Act.

DISCLAIMER

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata I Ahmedabad

www.argus-p.com

Key Contacts for the Data Privacy and Technology Practice

Vinod Joseph, Partner
vinod.joseph@argus-p.com

Udit Mendiratta, Partner
udit.mendiratta@argus-p.com

MUMBAI
11, Free Press House
215, Nariman Point
Mumbai 400021
T: +91 22 6736 2222

DELHI
Express Building
9-10, Bahadurshah Zafar Marg
New Delhi 110002
T: +91 11 2370 1284/5/7

BENGALURU
68 Nandidurga Road
Jayamahal Extension
Bengaluru 560046
T: +91 80 46462300

KOLKATA
Binoy Bhavan
3rd Floor, 27B Camac Street
Kolkata 700016
T: +91 33 40650155/56

AHMEDABAD
307, WestFace
Thaltej
Ahmedabad 380054
T: +91 79 29608450

www.argus-p.com I communications@argus-p.com