



**SEPTEMBER 2023
EDITION**

MONTHLY NEWSLETTER

**LEXTECH: CENTRE FOR
LAW, ENTREPRENEURSHIP
AND INNOVATION**



CONTENTS

1. Technology, Media and Telecommunications
2. Online Gaming and Betting laws
3. FinTech
4. Artificial Intelligence
5. Data Privacy

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS



SECTION 1



THE INDIAN TELECOMMUNICATION BILL 2022 – LEGAL IMPACT ON THE INDUSTRY

NEWS

The Union Cabinet has cleared the draft Indian Telecommunication Bill 2022, which contains certain relaxations in regulating communication services such as WhatsApp and Google Meet. The bill has been cleared by the parliament and may be introduced in the next session.

LEGAL TALK

The Draft Bill has expanded the definition of "telecommunication services" in clause 2(21) to include over-the-top ("OTT") communication services such as WhatsApp, Telegram, and others. This change subjects OTT services to the same licensing requirements as traditional telecommunications service providers ("TSPs"), despite their distinct software-based nature. OTT platforms offer voice calls and messaging that compete directly with TSPs but rely on the existing telecom infrastructure. This expansion aims to level the playing field between OTT providers and TSPs but has been met with opposition from those who argue that OTT services primarily use telecom infrastructure rather than providing telecommunications services themselves.

THE WAY FORWARD

The evolving landscape of communication services has led to discussions about the future of regulation. TRAI foresaw the possibility of telecom players becoming pure access providers with services offered by others. Recent recommendations from TRAI have recommended against regulating OTT communication services similarly to telecom services. This suggests a need for adaptable regulatory approaches to accommodate the changing communication landscape.



GUIDELINES FOR PREVENTION OF DARK PATTERNS

NEWS

The Department of Consumer Affairs (“DoCA”) has published draft guidelines for the prevention and regulation of dark patterns under the Consumer Protection Act 2019 (“CPA”). These define dark patterns as deceptive design patterns using user interface/user experience interactions on a platform to mislead or trick users into doing something they didn’t intend to do. For instance, a small, hard-to-spot “Unsubscribe” button hidden in an email is a tactic companies use to make cancellation difficult, indicating unfair trade practices.

LEGAL TALK

The CPA defines unfair trade practices as any act or practice that deceives, defrauds, or coerces consumers or exploits their vulnerability. This includes the use of dark patterns, which are deceptive design elements that trick consumers into making choices that are not in their best interests. Recently, the Advertising Standards Council of India (“ASCI”) released Guidelines for Online Deceptive Design Patterns in Advertising. These guidelines prohibit all advertisements that use misleading design patterns or that may be confused with editorial or organic content. The ASCI guidelines are the first concrete legislation in India to impose a blanket ban on dark patterns.



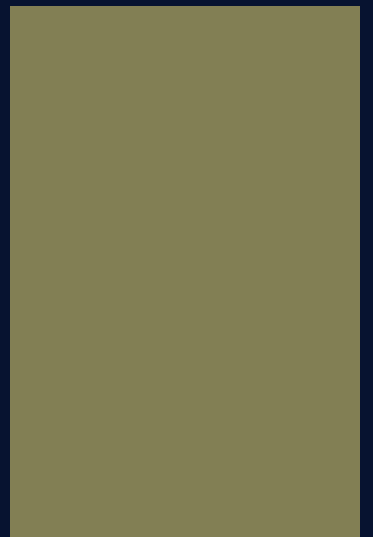
THE WAY FORWARD

In light of the new ASCI guidelines industry stakeholders, advertising agencies, and online platforms should actively engage in awareness and compliance efforts. Collaboration with consumer advocacy groups can aid in the dissemination of these guidelines and raise awareness about the importance of clear disclosure in advertising content. Moreover, the authorities should undertake a vigilant role in overseeing adherence to these guidelines and the CPA's provisions, taking appropriate action against violators. Strengthening consumer protection agencies and enhancing their investigative powers is a crucial step to bolster consumer rights.

Online Gaming and Betting Laws



SECTION 2



NEW ONLINE GAMING AND CASINO REGULATIONS: GST ON THE FULL COST OF THE CHIPS INITIALLY PURCHASED

NEWS

On September 6, the Ministry of Finance published a notification outlining changes to the GST regulations regarding online gambling and casinos. These changes mandate that everyone entering a casino must now pay GST on the entire amount of the chips they initially buy.

LEGAL TALK

The recent amendments to the Goods and Services Tax (“GST”) Act, 2017, have introduced two new clauses, 31B and 31C, which specifically address the computation of GST by casinos and internet gaming operators. These clauses require that the supply of services by casinos and internet gaming operators be valued based on the gross amount paid to the supplier by players, including any amount refunded to players. This means that GST is payable on the full amount paid to the supplier, even if any amount is refunded to the player. The impact of these amendments is that players will no longer be able to claim GST refunds on the refundable amount. This is because the supply of services by casinos and internet gaming operators is now considered to be a "taxable actionable claim" under the GST Act. This means that the GST liability arises on the sum paid to the supplier, regardless of whether any amount is refunded to the player or not.



THE WAY FORWARD

This new amendment has clarified how the value of supply should be computed by casinos and internet gaming operators. However, it remains unclear whether the simple act of depositing money into a wallet constitutes a supply under the GST law. This ambiguity could lead to disputes between businesses and the tax authorities. It is important for the government to issue a clarification on this matter.



BRAZIL'S LEGISLATURE APPROVES A BILL REGULATING INTERNET SPORTS BETTING AND GAMBLING

NEWS

The Brazilian lower house of parliament passed a landmark law governing online sports betting in the nation. The [bill](#) now enables the Brazilian government to levy an 18% tax on wagering and gaming. However, it should be remembered that only the net revenue a user generates will be taxed on the revenues from these activities. The Senate will now consider adding more formal clauses to the package. The businesses that will operate in Brazil will now need to apply for a grant. The grant's duration will be 36 months in total. Additionally, the cost to apply for a grant is 30 million Brazilian reals, or nearly \$6 million.

LEGAL TALK

The bill's passing represents the most recent milestone in the protracted process of regulating gambling in Brazil. Through Federal Law No. 13,756/18 by the Federal Senate, the government intended to control fixed-odds sports betting and gaming activities. Similarly, In India, the parliament proposed the "Online Gaming (Regulation Bill) 2022, which deals with the online gaming sector in India by setting up a commission to look after the same but the bill is not free of shortcomings the most prominent one is its does not classify between "games of skills" and "games of chance".

THE WAY FORWARD

The Brazilian government will be able to regulate the gaming and betting industry and collect taxes efficiently from this sector, which will aid in the country's further growth, thanks to the passage of this bill. It is also important to remember that it is illegal for anyone under the age of 18 to wager on athletic events. Additionally, those who are directly connected to a sporting event, such as athletes, coaches, and referees, are prohibited from participating in any form of gambling, with the exception of fixed odds betting.

DGGI DEMANDS A PAYMENT OF RS. 55,000 CRORE IN TAXES FROM DREAM11 AND OTHER ONLINE GAMBLING ENTERPRISES

NEWS

According to the sources, the Directorate General of GST Intelligence (“DGGI”) has written 12 pre-show cause notices to online real money gaming (RMG) organisations about GST obligations totaling nearly Rs 55,000 crore. These include what may be the biggest indirect tax notice ever served in the nation, a GST notice for over Rs 25,000 crore sent to the fantasy sports platform Dream11. The entire GST demand from RMG was raised by DGGI, and additional notices are anticipated in the upcoming weeks. The notices were sent out as a result of the recent change in GST rates for real money games, which raised the fee for each gaming session on RMG platforms from 2% to 28% of the entire bet.

THE WAY FORWARD

This GST demand can be detrimental to the online gaming industry that has been gaining traction in India for the first time, and the government and the respective authorities should not arbitrarily charge this kind of demand from these companies as this might lead to a strain in the relationship between online gaming companies and the Indian government, which will be detrimental for the Indian economy. Hence, the government should make decisions judiciously.



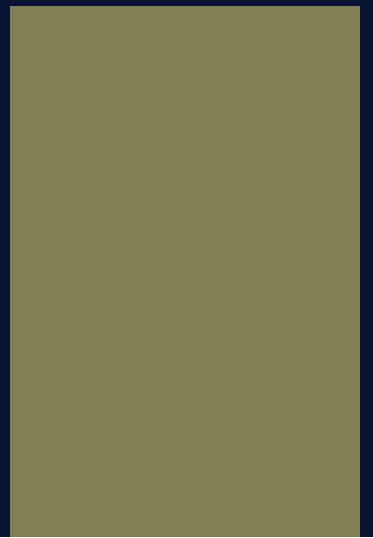
LEGAL TALK

The provisions relating to demand and recovery under the Goods and Services Tax (GST) Act, 2017, are set out in Chapter XV, Sections 73 to 84. Under Section 73, the proper officer may demand any tax, interest, or penalty that is due from a person under the Act. Under Section 76, a show-cause notice may be issued to a person who has not paid the tax to the government. If a show-cause notice is issued and the person disagrees with the demand made, they may appeal the decision to the adjudicating authority. The adjudicating authority is a quasi-judicial body that is responsible for resolving disputes between taxpayers and the tax authorities.

FinTech



SECTION 3



RBI PROPOSES A SELF-REGULATORY ORGANIZATION FOR FINTECHS



NEWS

The Reserve Bank of India (“RBI”) has asked FinTech entities to form a Self-Regulatory Organisation (“SRO”). SRO can help in establishing codes of conduct for its members that foster transparency, fair competition, and consumer protection.

LEGAL TALK

RBI has introduced a framework for the recognition of SROs under the Payment and Settlements Act, 2007. An SRO is an independent body that sets and enforces rules for its members, with the aim of protecting customers and upholding ethics and professionalism. SROs work collaboratively with all stakeholders to develop regulations and oversee their implementation. They employ impartial mechanisms to maintain discipline among members and enforce penalties when necessary. These mechanisms gain legitimacy through the mutual agreement of members and the effective administration of self-regulation.



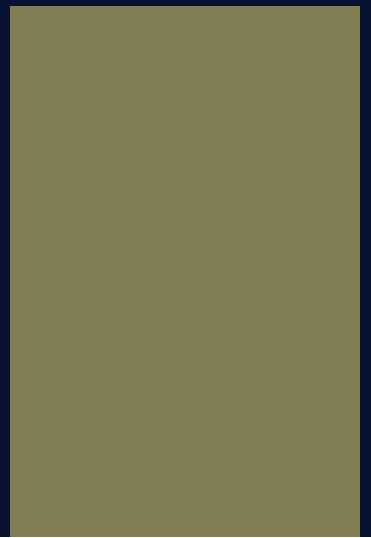
THE WAY FORWARD

SROs can play a pivotal role in fostering responsible practices and ethical standards within the Fintech sector. The need for SROs is highlighted by instances of unethical conduct by some Fintech players, such as charging exorbitant interest rates and harassing borrowers. SROs can build trust among consumers, investors, and regulators, and promote a sustainable and reputable Fintech ecosystem by leveraging their industry expertise. They can also establish a uniform grievance redressal and dispute management framework across their members.

ARTIFICIAL INTELLIGENCE



SECTION 4



GOOGLE LAUNCHES NEW TOOL TO DETECT ARTIFICIAL INTELLIGENCE ('AI') IMAGES

NEWS

DeepMind, in partnership with Google Research, launched its watermark tool, SynthID. Watermarks have long been used on paper documents and currency notes as a method of labelling them as authentic. With AI-generated images becoming more realistic, it is increasingly difficult to distinguish these from the real ones, and their quick identification is crucial.

LEGAL TALK

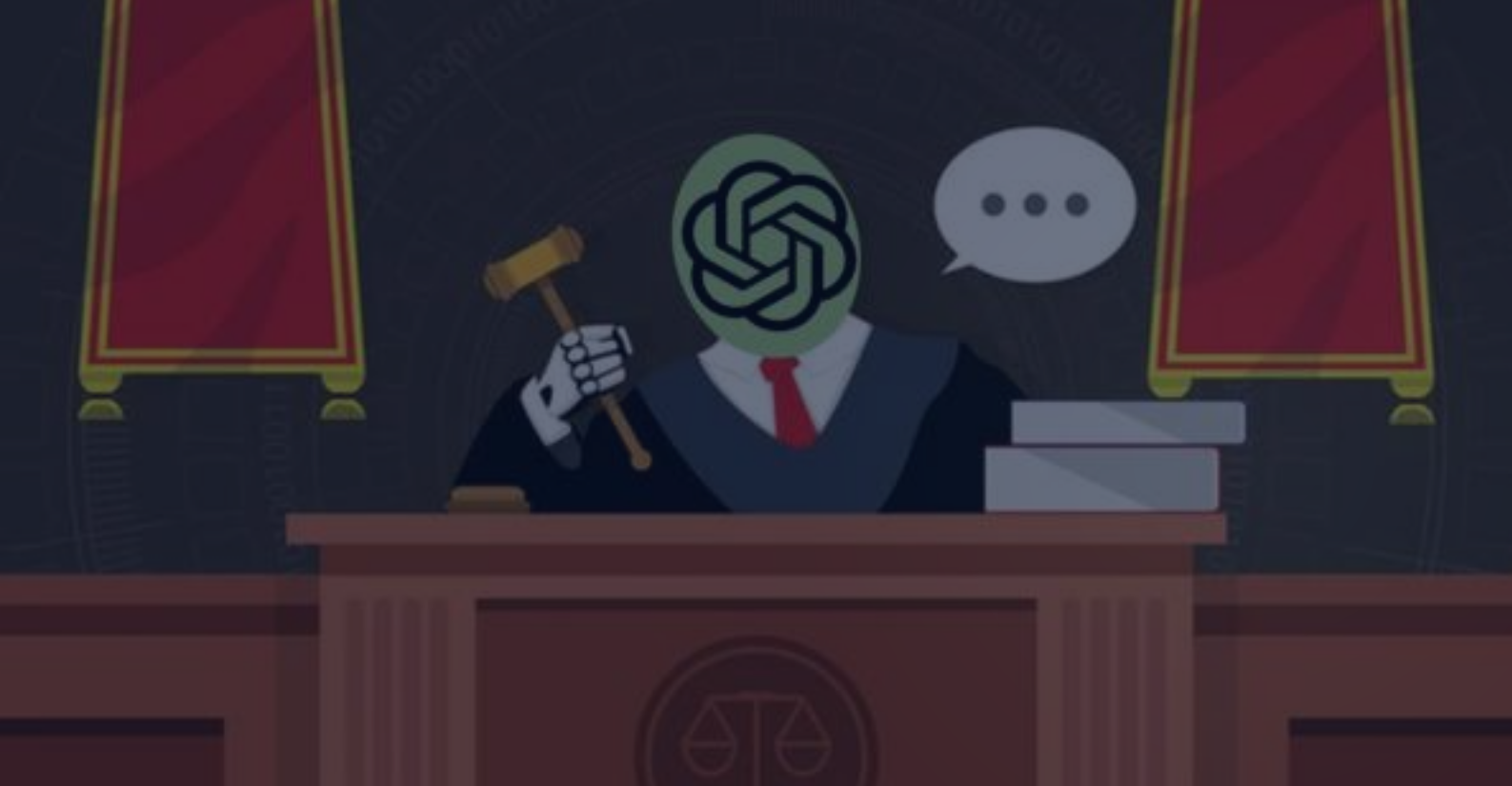
SynthID is a digital watermarking technology that creates hidden watermarks on images. These watermarks are imperceptible to the human eye but can be detected using special tools. SynthID can be used to identify images that have been created using AI tools. This is important because it can help to ensure that copyright is not granted to AI-generated works, which are not considered to be creative products of an author. Copyright is a legal right granted to creators of original works. Under Section 2(d) of the Copyright Act of 1957, an author is defined as a person who causes the work to be created (human or legal entities).

This definition excludes AI systems from being considered authors of AI-generated works. In other words, SynthID can help to protect human creativity and authorship by ensuring that AI-generated works are not granted copyright protection. This is important because it helps to ensure that human creators are fairly rewarded for their work and that AI is not used to create counterfeit or plagiarized works.

THE WAY FORWARD

Though the launch of the tool is experimental and DeepMind acknowledges that the tool may not be completely foolproof against extreme manipulation, it has the potential of helping prevent misinformation, cyber frauds, and copyright infringement. It would in any chance serve as a potential tool to help in protecting copyright-protected images and in preventing cyber frauds by helping people identify inauthentic images.





CAN AI SUBSTITUTE HUMAN INTELLIGENCE IN ADJUDICATING CASES: DELHI HIGH COURT ('HC')

NEWS

The single bench of Delhi HC in Christian Louboutin Sas & Anr v. Shoe Boutique, held that ChatGPT cannot substitute human intelligence in the adjudicatory process, as it responds differently to a command placed differently.

LEGAL TALK

The issue mentioned above came to light when the French fashion label Christian Louboutin used the responses from ChatGPT to support its arguments on the design infringement by the Indian brand Shoe Boutique. The HC before refusing to accept the response, tried to give a different prompt to the ChatGPT, an AI bot, and received a different response. It thus came to a conclusion that these AI-generated arguments are influenced by the user inputs, which are open to manipulation leading to biases. The courts refused to rely on them in the legal proceedings. The court further held that AI-generated responses are comprehensive overviews and should not be considered as opinions on the merits of a case. The court concluded that, at this stage, AI cannot replace the adjudicatory process.

THE WAY FORWARD

The High Court's decision is significant because it raises important questions about the reliability and admissibility of AI-generated evidence in court. On the one hand, AI tools can be used to generate comprehensive overviews of complex legal issues, which can be helpful to judges and lawyers. On the other hand, AI tools are susceptible to manipulation and bias, and their outputs should not be given the same weight as human-generated evidence.

ADOBE'S PROPOSAL OF ANTI-IMPERSONATION RIGHTS AGAINST GENERATIVE AI

NEWS

Recently, Adobe has proposed to the United States Congress that they establish a new Federal Anti-Impersonation Right Act ("FAIR Act") in light of developing AI and its ability to impersonate the works of original creators. It focuses on intentional impersonation for commercial gain.

LEGAL TALK

Artificial intelligence ("AI") poses a significant challenge to creative professionals. AI can be trained to generate new works in the same style and form as the original creators, but these style copies cannot be copyrighted. This leaves original creators exposed and vulnerable to economic harm. This impersonation of the style of an artist has been causing serious economic repercussions to the creator. The introduction of the FAIR Act can place the creators of original work in a better position. The following are the key insights of the proposal:

- 1) This would apply to the AI-generated work alone.
- 2) This would create the liability for the misuse of AI tools.
- 3) This would look into the intention to impersonate to create liability.
- 4) This would prevent someone's likeness of work from being licensed without the permission of the original creator.

THE WAY FORWARD

Companies can be encouraged to train AI systems using only licensed works, rather than original works. This would minimize the risk of copyright infringement. However, this would require collaboration between the industry and the government to ensure that AI technology is developed and deployed in a fair and reasonable way.



DATA PRIVACY



SECTION 5





INTERNET GIANTS SEEK EXTENDED TRANSITION FOR DPDP ACT COMPLIANCE ON CHILDREN'S DATA

NEWS

The Minister of State for Electronics and Information Technology anticipates that the implementation of the majority of the requirements outlined in the Act, except those about age-gating and similar aspects, to be completed within a span of 12 months. The government has been requested by social media platforms and prominent internet corporations to grant an extended transition period to guarantee adherence to the intricate stipulations outlined in the [Digital Personal Data Protection \("DPDP"\) Act](#).

LEGAL TALK

Section 9(1) of the Digital Personal Data Protection Act 2023 (DPDP Act) requires parental authorization for the processing of personal data on individuals under the age of 18. This requirement could impose significant burdens on young adults and adolescents, thereby impeding their unrestricted access to the Internet. At present, individuals who have reached the age of 13 or above are eligible to create accounts on several social media platforms, including Facebook, Instagram, YouTube, Twitter, and Snapchat. This is due to the legal provisions in the United States that permit the processing of data about individuals beyond the specified age threshold, particularly youngsters. The [General Data Protection Regulation](#) of the European Union explicitly identifies individuals under the age of 16 as children and grants member countries the option to lower the age of consent to 13 years, should they want to do so.

THE WAY FORWARD

A prospective course of action may entail the incorporation of a stratified and risk-dependent approach within the DPDP Bill to address the matter of children's data. Instead of mandating a uniform age-gating policy, it is proposed that the government be vested with the discretion to lower the age threshold for particular digital services that are devoid of significant privacy implications. These services encompass web search engines, online encyclopedias, and analogous platforms predominantly employed by minors for educational purposes. Conversely, stringent age-gating mechanisms may be instituted by video-streaming or e-commerce enterprises.



CREATION OF A DATA PROTECTION BOARD ('DPB') UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 ('DPDP ACT')

NEWS

Section 18 of the new DPDP Act establishes a Data Protection Board. The Board, as prescribed by this Act, will be a legal entity with perpetual existence, possessing the capability to own property, enter contracts, and undertake legal actions under its name.

LEGAL TALK

Despite appearing to grant increased authority, the DPDP Act 2023 designates the position of a chairperson for overseeing DPB decisions, while assigning the DPB the role of enforcing data protection by including investigations and levying penalties in line with the provisions of the DPDP Act. It is imperative to meticulously examine the practical implementation of the DPB's powers, as they endow the DPB with quasi-judicial prerogatives, similar to that of a civil court. This empowers the DPB to compel individual cooperation, scrutinize documents, and, when deemed necessary, enlist the assistance of law enforcement agencies for investigative purposes. Further, the act designates the Telecom Disputes Settlement and Appellate Tribunal ("TDSAT") as the appellate authority for challenges to decisions of the Data Protection Board (DPB). This means that if a Data Fiduciary is unhappy with a decision made by the DPB, it can appeal that decision to TDSAT. In addition, the DPDP Act gives the Central Government the power to shut down problematic applications or services, on the recommendation of the DPB. This power is only available in cases of recurrent violations of the DPDP Act. The Central Government's power to shut down applications or services is a significant one, and it is important to note that Data Fiduciaries could face serious business disruptions if they are found to be in recurrent non-compliance with the DPDP Act.

THE WAY FORWARD

Moving forward, it is crucial to strike a balance between enforcing data protection effectively and ensuring that the powers granted under the DPDP Act are exercised judiciously. A clear framework for the practical implementation of the DPB's authority must be established, including safeguards to prevent misuse. Additionally, transparent procedures for appeals, such as those involving the TDSAT, should be refined to ensure a fair and timely resolution. Businesses should prioritise compliance to avoid severe penalties and potential disruptions, emphasising the importance of robust data protection measures in the digital era.

CONTRIBUTORS

DESIGNERS

SAMRIDHI BAJORIA

NAMAN OSTWAL

TRISHNA AGRAWALLA

WRITERS

SHLOKA MATHUR

NAYANA KB

LAVANYA CHETWANI

ANJALI PANDE

TRISHNA AGRAWALLA

KUSHAL AGRAWAL

GARGI AGNIHOTRI

UTSAV BISWAS

EDITORS

NIKHIL JAVALI

HARSH MITTAL

**LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP
AND INNOVATION**

CONTACT US:



[INSTAGRAM](#)



[LINKEDIN](#)



[EMAIL](#)