LEXTECH

INSTITUTION'S INNOVATION COUNCIL
(Ministry of Education Initiative)

NOVEMBER 2024 EDITION

MONTHLY NEWSLETTER

LEXTECH: CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

NATIONAL LAW UNIVERSITY ODISHA

सत्ये स्थितो धर्म

CONTENTS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

SECTION 1

DOT DE-LINKS IN-FLIGHT WI-FI SERVICES FROM ALTITUDE RESTRICTIONS

NEWS

The Department of Telecommunications ('DoT') has amended the Flight and Maritime Connectivity Rules, 2018, through the Flight and Maritime Connectivity (Amendment) Rules, 2024. The amendment de-links Wi-Fi services from any altitude-based restrictions, allowing internet access whenever passengers are permitted to use electronic devices.

LEGAL TALK

The DoT, in pursuance of the Telecom Regulatory Authority of India ('TRAI')'s recommendations on In-Flight Connectivity ('IFC') from 2018, had introduced the rules in 2018. This paved the way for in-flight mobile and Wi-Fi services and also set out the standards for communication and compliance. The new amendment provides more clarity on the availability of Wi-FI services in aircrafts due to increasing demand for such services. Previously, Rule 9(1) of the 2018 rules allowed the operation of mobile communication services in aircrafts after it reached a minimum altitude of 3,000 meters to prevent interference with terrestrial networks. Rule 9(2), pertaining to internet services through Wi-Fi, was ambiguous in not providing an explicit altitude requirement. The updated rules align with the TRAI's 2018 IFC recommendations, which had emphasized that Wi-Fi services aboard aircraft do not pose the same risks of interference as mobile communication services, and that similar altitude requirements should not apply to in-flight Wi-Fi connectivity. Consequently, the amendment in Rule 9(2) has clarified the ambiguity of altitude requirements for Wi-Fi services and de-links Wi-Fi services from any altitude requirement, while retaining the 3,000-meter limit for mobile communication services.

THE WAY FORWARD

The amendment paves the way for significant changes in passenger experience by enabling seamless internet connectivity. However, the successful implementation of this change hinges on collaborative efforts among airlines, telecom providers, and regulators. Airlines may need to invest in robust satellite and ground-based systems to ensure reliable service. Additionally, DoT and TRAI should establish supplementary guidelines focusing on passenger data security, transparent terms of service, and measures to prevent cyber threats during flights. Balancing affordability with operational feasibility will be crucial to making in-flight Wi-Fi widely accessible across domestic routes. Airlines like Vistara were already offering limited in-flight Wi-Fi on specific routes. With this amendment, competitors like IndiGo and SpiceJet may follow suit, promoting wider adoption across the industry.

DOT RELEASES NEW CYBERSECURITY RULES

NEWS

The Department of Telecommunications ('DoT') has issued new Cybersecurity Rules ('The Rules') under the Telecom Act, 2023. These rules empower the government to request telecom traffic data, excluding message content, to enhance cybersecurity. Telcos are required to adopt robust cybersecurity policies, conduct audits, and report incidents promptly. The rules also mandate compliance mechanisms, including setting up Security Operation Centres ('SOCs') and ensuring the security of telecom networks.

LEGAL TALK

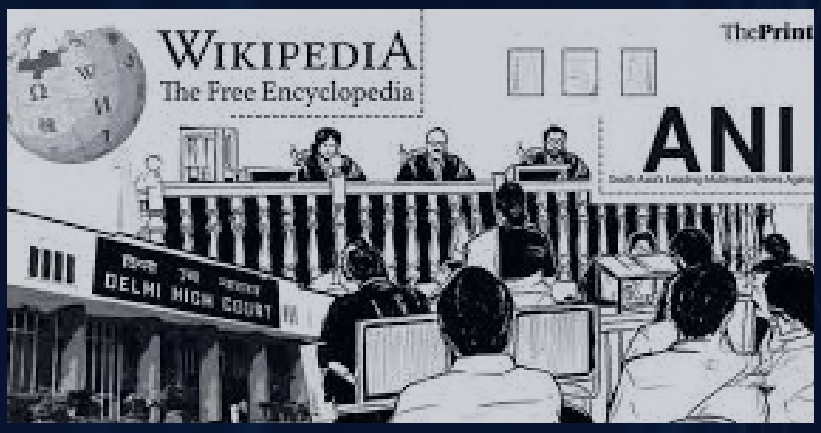
The newly notified rules under the Telecom Act introduce significant updates while retaining some aspects of the draft rules introduced in August. Notably, the exemption of message content from government access is a major change from the draft version, reflecting a conscious effort to address privacy concerns. The rules mandate telecom companies to adopt cybersecurity policies, conduct periodic audits, and report incidents promptly, but now allow a more extended timeline for furnishing detailed incident reports in twenty-four hours instead of six hours.

Key measures retained from the draft rules include requiring telecom companies to establish SOCs, appoint a Chief Telecommunication Security Officer ('CTSO'), and conduct audits through certified agencies. Provisions to disconnect telecom identifiers of threat actors, register equipment with tampered IMEI numbers, and ensure compliance via secure communication channels also remain unchanged. These new changes aim to strike a balance while addressing privacy concerns raised in the earlier draft.

THE WAY FORWARD

The Rules underscore India's dedication to fostering a secure and robust telecom ecosystem. By implementing stringent safeguards, establishing accountability through the CTSO, and utilizing advanced digital tools, these rules effectively tackle the increasing complexity of cyber threats in the telecom sector. As India advances in its digital transformation, these regulations play a vital role in safeguarding users and enhancing trust in the nation's telecommunications infrastructure. Additionally, extending these provisions to cover OTT services in the future can enhance cybersecurity comprehensively, given their prevalence in communication. India should also align its rules with global best practices, fostering international cooperation on cybersecurity standards. Regular assessments and updates to the rules will ensure they remain relevant. By adopting a balanced and inclusive approach, the government can achieve robust telecom security without compromising innovation or privacy.

ANI V WIKIMEDIA FOUNDATION: DELHI HC CRACKS DOWN ON WIKIPEDIA CONTENT FOR ALLEGEDLY VIOLATING THE SUB JUDICE RULE



NEWS

The Delhi High Court has directed the Wikimedia Foundation to take down specific pages and discussions on Wikipedia that allegedly interfere with court proceedings and violate the sub judice principle.

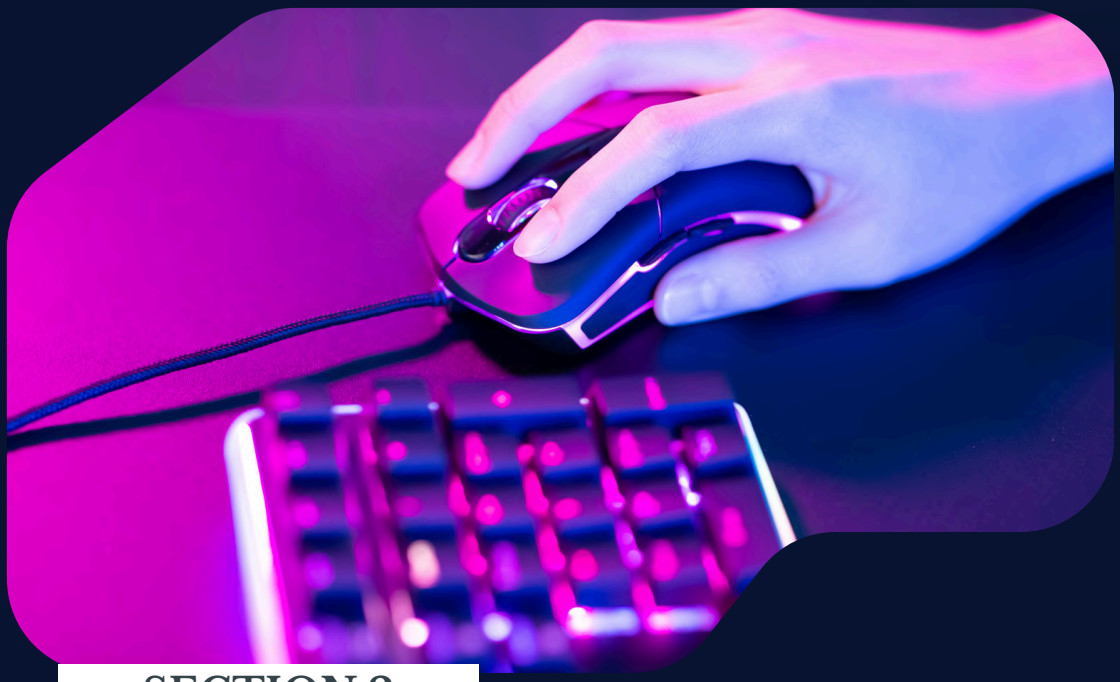
LEGAL TALK

During a recent hearing, the Court noted that comments on an earlier order requiring disclosure of Wikipedia editors' identities in a related case had been published on the platform, labelling the order as "censorship" and a "threat to the flow of information". The Court found such remarks and subsequent discussions on the matter to be a potential interference in judicial proceedings, especially given Wikimedia's status as a party in the suit. Following this, Wikimedia backed down and agreed to serve summons to the three editors implicated in the suit and file a sealed affidavit disclosing their subscriber details, per the latest order. It is interesting to recall the Neetu Singh v. Telegram FZ LLC case at this point, where Justice Pratibha M Singh compelled Telegram to disclose user data, including IP addresses and email IDs, of those accused of sharing copyrighted educational content without authorization. The Court rejected the privacy argument, stating such protection cannot shield unlawful activities in the name of privacy. Telegram, known for its anonymity, complied with the order, a decision that set a significant benchmark for addressing online misuse. The High Court passed a similar direction for disclosure to Facebook and Telegram in a venture capital firm's case this year. Meta later complied with the order. However, the root of the matter goes back to a lawsuit filed by ANI against Wikipedia for allegedly hosting defamatory content in which they have demanded INR 2 crores in damages and removal of certain content. ANI has contested the description of it as a mouthpiece of the Central government on its Wikipedia page, with the Division Bench appearing to agree that it is defamatory. Wikipedia currently benefits from safe harbour protection under the Information Technology Act, 2000 ('IT Act'), shielding it from liability for user-generated content. However, the Intermediary Guidelines, 2021 ('IT Rules, 2021') mandate that platforms like Wikipedia must make a "reasonable effort" to prevent the dissemination of illegal content. Wikipedia's appeal initially focused on requesting reasons for disclosing its user information, but it has escalated into a matter that could jeopardize its operation in India. On September 5, Justice Chawla warned of potential government action to shut down the platform for failing to comply. The Division Bench also cautioned that Wikipedia's appeal could endanger its intermediary protection under Section 79 of the IT Act, especially since it defended content on ANI's page despite being only an intermediary. The Court emphasized that users responsible for the edits must defend themselves, while the original sources are not part of ANI's suit.

THE WAY FORWARD

Wikipedia's defence rests on its identity as a collaborative platform. It is a free online encyclopedia edited by volunteers, who research, summarize, cite sources, and update articles on the website. Some pages are protected, allowing edits only by administrators chosen for their contributions. Administrators handle advanced tasks like deleting pages and blocking users. While Wikimedia provides the platform's infrastructure, it does not edit content or define volunteer roles. This distinction underpins Wikipedia's claim that it functions as a platform, not a publisher. Unlike copyright infringement or fraud cases, the Wikipedia dispute touches on broader user privacy issues and freedom of speech. Academics have cautioned against the chilling effect such actions could have on contributors who participate in the dissemination of knowledge. Wikipedia is not merely a platform but a global movement advocating free access to information and fostering dialogue in an increasingly polarized world. There have been warnings that censorship or punitive measures against critical content could stifle the ideals of free speech and discourage future contributors.

Online Gaming and Betting Laws



SECTION 2

GAMING REGULATION UNVEILED: STRIKING A BALANCE BETWEEN STATE CONTROL AND NATIONAL FRAMEWORKS

NEWS

At the recent India Gaming Convention 2024 in New Delhi, Md. Nasimuddin, IAS (Retd.), Chairperson of the Tamil Nadu Online Gaming Authority ('TNOGA'), took part in a significant panel discussion on "Guardians of the Game: Balancing Benefits and Safety in Gaming for Minors" and addressed the concerns over the jurisdictional limit of states in handling the menace of offshore betting and gambling platforms. He emphasized the importance of data-driven regulation in the gaming industry.

LEGAL TALK

As per the Constitution of India, it is the states that have the authority to make laws for controlling betting and gambling (Entry 34, List II of the Seventh Schedule). This in turn empowers Tamil Nadu to pass enactments that are aimed at controlling online gaming in the state. However, limitations come in when dealing with international operators as states are unable to exert authority outside the borders of India. Any such regulation of these platforms would have to take into account the Central government which is vested with power in relation to "interstate trade and commerce" (Entry 42, List I) and "communication" (Entry 31, List I) among other subjects. The Centre in such cases may take further steps by adopting enabling provisions such as the Information Technology Act, 2000 or by making a national regulatory framework to ensure that there is no disparity in regulation across states. An additional dimension to regulatory enforcement is given with Nasimuddin's proposal of participation of Internet Service Providers ("ISPs"). ISPs may usefully assist in blocking access to illegal gaming sites in terms of the provisions of the Information Technology (IT) Act, 2000, Section 69A, that allows the Government of India to control distribution of information for the sake of protecting the public. Nevertheless, burdening this duty backfires the concerns on the intermediary liability in section 79 of the IT Act where ISPs cannot be held liable for third-party contents when they adhere to the guidelines.

THE WAY FORWARD

A robust way forward involves a collaborative approach between the Centre, states, ISPs, and gaming stakeholders. The Centre should establish a unified national framework under the IT Act, 2000, addressing offshore gaming platforms and harmonizing state-level laws. ISPs can play a critical role in enforcing Section 69A directives to block illegal platforms, but this must be balanced with intermediary liability protections under Section 79. States like Tamil Nadu should focus on data-driven regulations and stakeholder consultations to craft effective policies. Encouraging self-regulation through industry codes of ethics and raising public awareness about responsible gaming will further ensure a safer ecosystem.

FinTech

SECTION 3

U.S. CONSUMER FINANCIAL PROTECTION BUREAU FINALIZED THE RULE TO TO SUPERVISE BIG TECH PAYMENTS, DIGITAL WALLETS

NEWS

The U.S. Consumer Financial Protection Bureau ('CFPB'), has finalized the rule which aims to supervise big tech companies operating in the payments and digital wallets space. The significant regulatory development brings several digital payment platforms and digital wallets—offered by tech giants such as Apple Pay, Google Pay, and PayPal—under the CFPB's direct oversight.

THE WAY FORWARD

The rule is set to take effect 30 days after its publication in the Federal Register. This timeline allows companies time to prepare for compliance. The CFPB's new rule represents a pivotal moment in the regulation of digital payments in the U.S., aiming to create a safer, more transparent environment for consumers while holding major tech firms accountable. By establishing a framework for the supervision of these entities, the CFPB aims to enhance consumer protection by ensuring that these platforms adhere to federal consumer financial laws, promoting transparency and fairness in financial transactions. This regulatory move also raises questions about the balance of power between federal oversight and state regulations, as the CFPB's actions could preempt certain state laws unless they offer greater consumer protections. The development is expected to provoke legal challenges from industry stakeholders who argue that such oversight could stifle innovation and competition within the rapidly evolving fintech sector.

LEGAL TALK

The rule is part of the broader regulatory framework established under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which created the CFPB to enforce federal consumer financial laws and protect consumers in financial transactions. The final rule will enable the CFPB to supervise key areas in the digital payment sector which include:

1. Privacy and Surveillance: Tech companies collect vast amounts of transaction data. While federal law allows consumers to opt out of certain practices and prohibits false claims about data protection, concerns about misuse remain.

2. Errors and Fraud: Consumers have the right to dispute incorrect or fraudulent transactions under federal law, but many payment apps push dispute resolution onto banks and credit card companies. This is especially troubling for older adults and servicemembers vulnerable to scams.

3. Debanking: Losing access to payment apps without warning can disrupt consumers' lives significantly. Users have reported issues with account freezes or closures, causing payment disruptions and financial stress.

In addition to general-use digital consumer payment applications, the regulations also cover digital transactions involving consumer financial products or services such as the origination, brokerage, or servicing of real estate-secured loans, mortgage loan modifications or foreclosure relief services, private education loans, and payday loans.

The initiative represents a significant shift in the regulatory landscape, marking the extension of financial oversight to non-traditional players in the payment space. It empowers the regulator to conduct internal scrutiny of the respective digital payment applications and check for legal compliances.

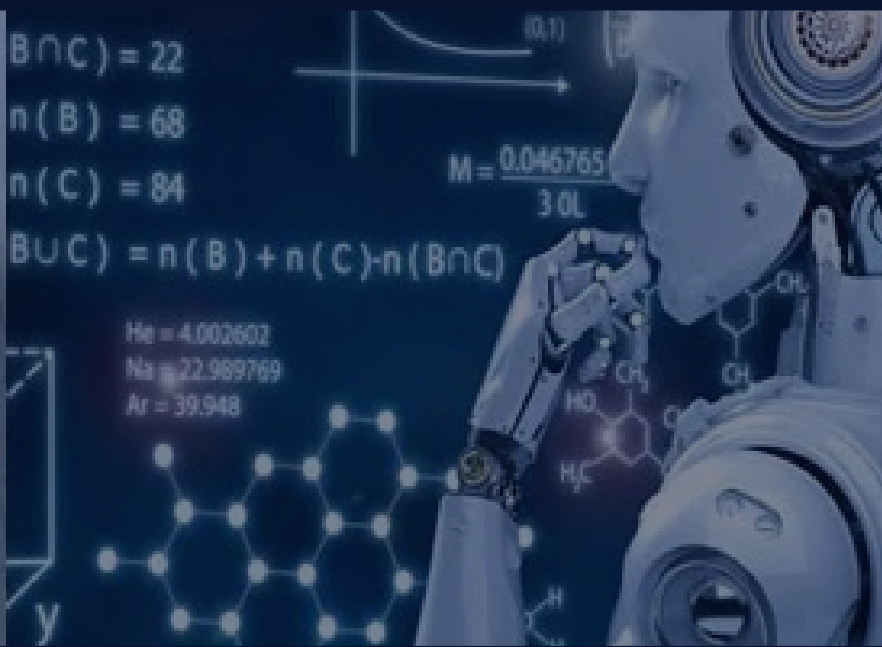
SEBI RELEASES NEW GUIDELINES TO REGULATE USE OF AI/ML IN FINANCIAL MARKET

NEWS

Securities and Exchange Board of India's ('SEBI') new guidelines impose stricter regulations for the use of Artificial Intelligence/ Machine Learning in financial markets to increase accountability among intermediaries such as brokers, mutual funds, and other participants across the financial markets. The guidelines intend to mitigate risks from algorithmic failure, data breaches, and systemic threats while ensuring compliance with investor protection norms. Entities that use AI/ML shall have to provide for appropriate measures for data privacy, system transparency, and regulatory compliance, and SEBI may impose suitable penalties in case of default.

LEGAL TALK

SEBI's proposed framework addresses critical gaps in the existing regulatory environment relating to AI/ML systems in financial markets. The liability of intermediaries, even for third-party systems, dispels ambiguity surrounding the issue of accountability and establishes clear legal recourse for investor harm. This approach is consistent with established principles of fiduciary duty and ensures that entities cannot disclaim responsibility for AI-related failures. Integrating data privacy obligations under the DPDP Act complements this framework, but its interplay with SEBI's specific rules raises questions about overlapping compliance burdens. SEBI's mandate for system audits and transparency appears legally sound, aligning with global standards like the EU AI Act, which prioritizes algorithmic fairness and explicability. However, the lack of provisions for AI-specific issues, such as unintentional regulatory breaches by self-learning algorithms, may require future refinements to ensure comprehensive governance. Further, the framework's emphasis on preventing systemic risks in algorithmic trading underlines the need for proactive oversight. This may take the form of improved market surveillance or clearer reporting obligations. While these improve investor confidence, their implementation may disproportionately impact smaller entities, potentially raising questions about proportionality under principles of equity in regulatory design. Ultimately, this will be a forward-looking attempt by SEBI to regulate AI/ML in financial markets, however, its legal robustness would depend on striking a balance between stringent compliance expectations and fostering innovation and fair competition.



THE WAY FORWARD

To comply with SEBI's directives, financial market participants may need to invest in advanced oversight frameworks, including routine audits, AI model validation, and stakeholder training. Policymakers should also consider introducing collaborative mechanisms between entities and regulators to refine the framework. By maintaining a delicate balance between investor protection, innovation, and cost-effectiveness, SEBI's approach could set a precedent for responsible AI integration in financial systems. Regular reviews and harmonization with global best practices will be crucial to the framework's success. Financial market participants may need to invest in advanced oversight frameworks to comply with SEBI's directives. These may include routine audits, AI model validation, and stakeholder training. Policymakers should also consider introducing collaborative mechanisms between entities and regulators to refine the framework. By maintaining a delicate balance between investor protection, innovation, and cost-effectiveness, SEBI's approach could set a precedent for responsible AI integration in financial systems. Regular reviews and harmonization with global best practices will support the framework's success.

RBI'S NEW ACCESSIBILITY GUIDELINES: A STEP TOWARD INCLUSIVE DIGITAL PAYMENT SYSTEMS

NEWS

The Reserve Bank of India ('RBI') has taken a significant step toward fostering inclusivity in digital payment systems by releasing new guidelines aimed at improving accessibility for the specially-abled. These guidelines mark a significant step in the digital payment sector, reflecting the growing reliance on these platforms for daily financial transactions.

LEGAL TALK

The guidelines highlighted the need for Payment system participants ("PSPs") such as banks and authorized non-bank providers are required to evaluate their systems. This review aims to identify areas where accessibility enhancements are needed, and thereafter modify these systems to ensure seamless use. All modifications must be in line with the Accessibility Standards and Guidelines for Banking Sector issued by the Ministry of Finance earlier this year, as well as RBI's Master Circular on Customer Service in Banks released back in 2015, both of which emphasise the need to cater to diverse disabilities without compromising user-friendliness. PSPs have also been tasked with balancing accessibility enhancements with the integrity and security of payment systems. The RBI emphasizes that these modifications must maintain robust security measures to safeguard user data and ensure secure transactions. Additionally, PSPs must submit a detailed report to the RBI within a month of the release of guidelines. This report should outline the required changes, provide a time-bound implementation plan, and include the contact details of a designated nodal officer, ensuring accountability and effective monitoring of progress. While the guidelines are well-intentioned, their execution may pose challenges. Adapting existing systems to meet accessibility standards may involve significant technical overhauls. For instance, ensuring compatibility with screen readers, voice recognition, or tactile feedback mechanisms might require substantial investment and time. Further, striking a balance between cost and compliance may be difficult, especially for smaller entities with limited resources. Finally, the effectiveness of the initiative will depend on the robustness of the RBI's monitoring mechanisms. Without consistent follow-ups and penalties for non-compliance, implementation could lag.

THE WAY FORWARD

The emphasis laid by the guidelines on inclusivity demonstrate the RBI's commitment to making financial services universally accessible and reinforces the broader goal of equitable financial inclusion. By focusing on the needs of the specially-abled, the RBI seeks to bridge the gap that often excludes individuals with disabilities from fully participating in the digital economy. While challenges in implementation are inevitable, the long-term benefits of inclusion, innovation, and equitable access outweigh the initial costs and efforts. With effective execution, this initiative can set a global benchmark for accessibility in digital financial services.

ARTIFICIAL INTELLIGENCE

SECTION 4

ANI VS OPENAI: SPECULATING CHATGPT'S POSSIBLE STANCE

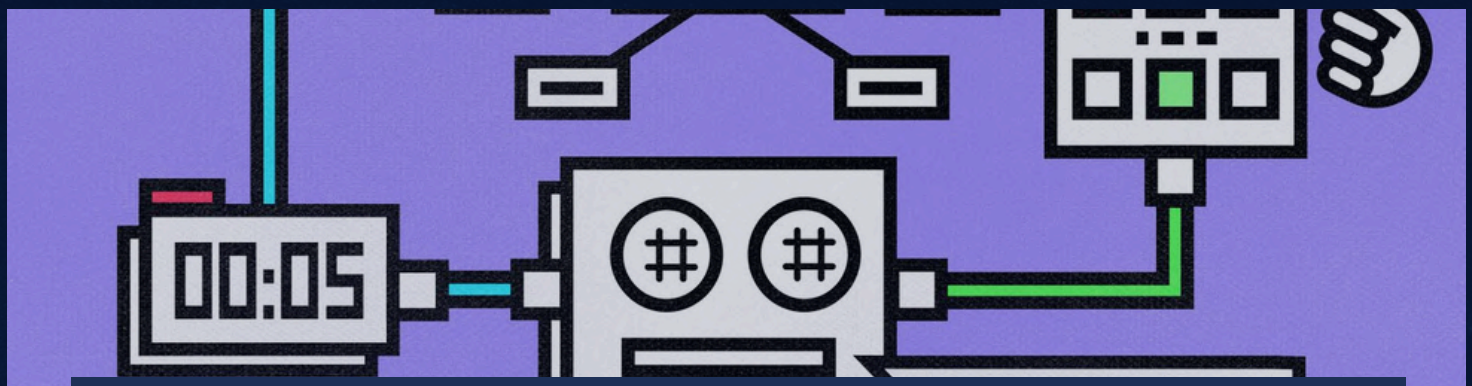
NEWS

In a recent development, Asian News International ('ANI'), an Indian news agency, functional through blogs and social media content, has brought the Chat-GPT parent OpenAI to court regarding copyright infringement. The allegations, while first in India, find concurrence with lawsuits filed in over 13 jurisdictions against OpenAI, especially with what is considered as the umbrella of this series, the New York Times vs OpenAI tussle. ANI contests that OpenAI has breached their copyright by violation of section 14 and 16 of the Indian Copyright Act, 1957. The key issues raised by ANI pertain to training of AI models feeding on its data, Chat-GPT producing verbatim results as ANI reports and lastly wrongly attributing things to ANI. The proceedings initiated in the Delhi High Court shall continue on 28th January 2024, where OpenAI has been asked to furnish a detailed response to ANI's accusations, in the first proceeding on 19th November 2024. In an interesting adjacent development, on 7th November 2024, a New York federal judge gave a rare green flag to OpenAI in summary dismissal of a lawsuit brought by Raw Story and Alternet, news organizations who had similar allegations as ANI.

LEGAL TALK

With the premise that the allegations running in multiple of such suits is essentially the same, it becomes important for us to understand what was held in the New York decision and what it holds for legitimizing generative AI.

The claim of Raw story in its suit was that OpenAI violated the U.S.C. § 1202(b)(1) – an element of the Digital Millennium Copyright Act ('DMCA') that prohibits intentional removal or alteration of copyright management information ('**CMI**'). While some opinions say that this was a weak claim in itself, due to its silence on the direct aspect of copyright infringement, nevertheless the reasoning that the court took holds importance. While considering the question of whether an injunctive relief should be granted to Raw Story, the court was assessing whether OpenAI garners 'Substantial Risk' in the light of the material on record. The court notes that when a question is asked to Chat-GPT it looks into its repository and synthesises relevant information into an answer. Thus, given the huge information repository, there is a remote chance that the output plagiarized the plaintiff's content. The judge here gives AI the liberty of a human mind, which when reproducing learned knowledge, cannot be questioned for infringing copyright. This is severely inconsistent with the apparent US policy in granting copyright, where the Copyright board even rejects copyright to pieces with speculated AI assistance. It remains to be seen whether this stance lasts any longer in the US.



It is important to note that even OpenAI does not seem sure of this out of the blue decision. Instead it chooses to rely on the recently amended 'Opt-Out' Policy. In the latest amendment of 23rd October 2024, OpenAI modified the policy by removing the line, "We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services". Non-API content is the content external of what is directly fed into Chat-GPT by users, which is all of the data on the rest of the internet. This Opt-Out facilitates self-induced non-access to publicly available data of independent producers, by filling a simple form. However, Opt-Out is also not the final solution either, because in the larger picture, it is not the copyright that is in danger, it's the capacity of creation that AI targets. An interesting and extensive opinion on this regard is available on SpicyIP by Mr. Akshat Agrawal. Other initiatives also include Chat-GPT officially collaborating with news agencies via license to train the models on their content. With these developments, it appears that OpenAI is now stepping into a direction where they seek ease of doing business over ascertaining the appropriate legal status of their technology.

THE WAY FORWARD

These trends and the increasing lawsuits project that AI literacy has started coming into effect and even largely monopolistic players would also have to bend knees before the Legal Anvil. It is nobody's case that India should follow the suit of US or even that the US federal judge's decision stands, but it is important that while we may see short term benefits reaping out of exclusionary bending via license fees and other encumbrances, it must be a constant quest for courts, legal officers, lawyers and even learners of Law to find the solution to this legal puzzle.

DATA PRIVACY

SECTION 5

THE DPDPA ANGLE TO WHATSAPP'S CONTENTIOUS PRIVACY POLICY

NEWS

The Competition Commission of India ('CCI') recently passed a landmark order penalising WhatsApp for abusing its dominant position under Section 4 of the Competition Act, 2000. It had been closely monitoring the 2021 policy update which had faced severe backlash on its introduction. While the issue primarily revolved around privacy, the CCI emphasised that the policy's approach to data access also raises significant competition concerns.

LEGAL TALK

In 2021, WhatsApp updated its policy to allow the use of users' personal information without giving users the option to opt out. The platform announced it would send periodic reminders to accept the new policy and eventually limit functionality for those who refused. WhatsApp clarified that it does not read or share personal messages with its parent company, Meta. Instead, the update focused on optional business features. Businesses using Meta's hosting services for managing chats could access conversation data for purposes like customer support and marketing. These businesses may also use collected data to target users with ads on Meta platforms, such as Facebook and Instagram. After the CCI's order WhatsApp has stated that its update aimed to enhance transparency about data sharing practices and that no users lost access to services. This clarification, while timely, could have addressed concerns more effectively if shared back in 2021.

THE DPDPA PERSPECTIVE:

At first glance, the update appears to apply primarily to conversations with businesses, allowing WhatsApp to use data from these interactions for targeted advertising. Personal chats and data remain protected by end-to-end encryption. However, there are various concerns which have not been addressed yet. WhatsApp collects approximate location data using phone numbers and IP addresses. Marketing chats also include users' payment and transactional information which have details like shipping addresses - all of which can now be potentially used by businesses. The update places users in a "take-it-or-leave-it" scenario, compelling them to accept the terms without offering a meaningful choice to decline.

By sending persistent notifications asking users to accept the terms, WhatsApp creates an illusion of choice while effectively forcing compliance. Such tactics undermine the principles of free and informed consent, which are central to data protection regulations like the DPDPA. According to Section 6, consent must be explicit, freely given, and revocable, none of which is adequately addressed in WhatsApp's approach. Users are also not given the option to withdraw their consent or erase shared data. Children using shared accounts or devices may inadvertently have their data processed without parental consent. Additionally, targeted advertising directed at children is explicitly prohibited under the DPDPA, and any violation of this rule could attract significant penalties for the platform. People consenting to WhatsApp's terms are not explicitly consenting to individual businesses using their data. Each business should be treated as an independent data processor and held accountable and forced to fulfill its obligations under the Act. Customers may unknowingly share sensitive information, such as financial or health details, which could be used for profiling or invasive advertising. Small businesses often lack the resources to ensure secure data handling, exacerbating these risks. Simply displaying a notification asking users to accept the terms does not meet the requirements of informed consent. The policy does not clearly specify what data is collected or how it will be used, leaving users in the dark. This ambiguity directly conflicts with the transparency requirements outlined under Section 5.

Meta may assume it can avoid scrutiny because the DPDPA has not yet come into force. However, existing laws still protect user rights, and their provisions can hold entities accountable for privacy violations. Under Section 72 of the IT Act, 2000, any person who, by exercising powers granted under the Act, gains access to electronic records, books, correspondence, or other materials and discloses this information without consent is liable for punishment. Consent obtained through coercive tactics, such as negative reinforcement or persistent reminders, does not align with the genuine and informed consent envisioned by lawmakers. However, the IT Act's broader scope and general applicability make proving data misuse more challenging compared to the DPDPA's specific obligations.

LEGAL VALIDITY OF SUCH AN ACTION IN DPDPA'S ABSENCE:

What's interesting is that the practice of requiring users to consent to data processing or lose access to a service is not inherently illegal, provided certain conditions are met. Rule 3(1)(c) of the Information Technology Rules, 2021 grants intermediaries the right to terminate access or usage rights if users fail to comply with their privacy policy. This reflects the legislative intent to ensure adherence to privacy standards. While the constitutionality of these rules has been questioned in court, they remain enforceable until a judicial decision invalidates them. From a legal standpoint, such practices are permissible as long as users are informed transparently about what data is being collected, the purpose of its use, and the consequences of non-consent. In practice, similar arrangements exist worldwide. For example, under the General Data Protection Regulation in the European Union, data controllers must obtain explicit consent for data collection, but businesses can condition access to services on this consent if the data is necessary for the service. This viewpoint is supported by the acceptance of the "pay or consent" model by the European Data Protection Board. While there has been a lukewarm response and developing guidelines are still in progress, it indicates that regulators recognize the necessity of data processing for business operations and are attempting to balance the same with privacy requirements.

This aligns with the logic behind Rule 3(1)(c), suggesting that such conditions are acceptable if users are adequately informed. This approach is driven by the competitive nature of modern business and capitalistic markets which are the norm, where targeted advertising and data analytics are crucial for success. Data has become vital to the digital economy, enabling personalized services and innovation. Even if WhatsApp issued a clearer notice, the issue isn't that simple. While WhatsApp can restrict user access for non-compliance, it shouldn't do so for reasons unrelated to its core service, like messaging. Forced consent can unfairly disadvantage users, especially when alternatives are limited, raising fairness concerns. Courts may eventually rule on whether such practices exploit users, especially in monopolistic situations. Additionally, competition law regulators view these practices as an abuse of WhatsApp's dominant position.

THE WAY FORWARD

The CCI's decision is a win for data privacy, as it has instructed WhatsApp to stop sharing data with Meta and mandated clearer notices detailing what data is used for specific processing purposes. A decision under the DPDPA would likely have led to similar outcomes. Meta is facing increasing resistance in the European Union for its harmful policies, including backlash last year over requiring users to pay to avoid personalized ads. As regulators slowly work to balance business interests with data privacy, it's in Meta's best interest to adopt more user-friendly policies and offer real choices, given its weakening position globally.

BOMB HOAX INVESTIGATION STIFLED DUE TO PRIVACY CONCERNS

NEWS

India's pursuit of the perpetrators behind multiple bomb threats, which severely disrupted the country's aviation and hospitality sectors, has encountered resistance in Europe. Most of the hoax calls were reportedly routed through Virtual Private Networks ('**VPNs**') based in European nations. Countries like France and Germany have invoked provisions under the General Data Protection Regulation ('**GDPR**'), asserting that they require specific warrants identifying the perpetrators before they can advance the investigation.

LEGAL TALK

Over the past month, over 500 bomb threat calls to airlines and hotels across India, all hoaxes, have drawn attention to the misuse of VPNs. VPNs, which encrypt connections and mask IP addresses to protect user privacy, are often exploited for criminal activities. However, VPNs themselves are not inherently illegal. In India, VPN usage remains legal, but the regulatory landscape is uncertain. In 2022, CERT-In mandated that VPN providers store extensive user data for five years, including names, IP addresses, and usage patterns. Non-compliance could lead to penalties, including imprisonment. This rule contradicts VPNs' primary function of preserving privacy, potentially compromising over 270 million users' data and violating the principle of proportionality under the Indian Constitution. Most VPN providers adhere to strict no-logs policies, and many transactions occur through cryptocurrencies, making user tracking difficult. Critics argue that the government's assurance of case-by-case data requests fails to address concerns about surveillance of critics, activists, and politicians. The measure assumes anonymity equates to malicious intent, ignoring that most users employ VPNs for legitimate purposes, like data protection or bypassing geo-restrictions. Storing detailed logs won't deter cybercriminals, who can easily switch to alternatives like encrypted apps or proxy servers. Cybercrimes often stem from weak infrastructure and insufficient literacy, not VPN use. Instead of extreme measures, the government should enhance cybersecurity infrastructure, promote digital awareness, and secure data storage to address cybercrime without compromising user privacy. Forcing data retention increases risks of misuse or leaks, undermining the very principles VPNs are meant to uphold.

India’s approach to VPN regulation contrasts with Europe’s, where data autonomy and anonymity are prioritized. In Europe, exceptions for national security or foreign relations are sparingly invoked, with a higher burden of proof. The GDPR, through Articles 44 and 45, mandates that personal data of European residents must remain within Europe, barring transfer overseas without strict checks. While data sharing for national security is permitted within Europe, it remains unclear if the same applies to non-European nations' concerns. Europe’s measured approach ensures investigations do not unjustly compromise privacy, with mechanisms to inform non-perpetrators if their data is involved, allowing for potential legal recourse. Balancing legitimate data access with privacy requires robust cross-border data sharing frameworks. Unlike the U.S., which uses the CLOUD Act to access European data under specific conditions, India lacks such agreements with Europe. India has also refrained from joining the Budapest Convention on Cybercrime, citing concerns about disclosing sensitive national data. This limits its options to slow alternatives like the Mutual Legal Assistance Treaty or court-issued letters rogatory, which rely heavily on foreign cooperation. These methods highlight India’s challenges in securing timely access to international data while safeguarding privacy.

THE WAY FORWARD

VPN providers, linked to Big Tech firms, store data across global cloud servers, preventing India from directly accessing a specific user's data. If reversed, India would likely deny foreign data requests without clear warrants, especially for national security. With the DPDP Act nearing implementation, India could soon formalize laws to address cross-border data breaches. While GDPR protects non-perpetrators' data, national security investigations can justify exceptions. India and the EU could collaborate on data access in sensitive cases. India could benefit from signing such a treaty, provided it adopts a proactive stance like Europe in prioritizing data protection. India must adopt a more balanced approach, protecting citizen data while limiting government overreach. Its increasing tendency to grant unrestricted access to government bodies has undermined privacy, as seen in declining global freedom rankings. India should promote open cross-border data flow, improve post-attack responses, and focus on international cooperation, recognizing that it's impossible to fully prevent misuse. By safeguarding rights, India can better tackle cyber threats without infringing on freedoms.

CONTRIBUTORS

WRITERS

PRATYUSH SINGH

ANJALI PANDE

SOUVICK SAHA

SUBHASIS SAHOO

ANANYA SONAKIYA

MAITHILI DUBEY

ARUNIMA RAMAN

ALOK SINGH MOURYA

TRISHNA AGRAWALLA

EDITORS

HARSH MITTAL

LAVANYA CHETWANI

DESIGNERS

ARUNIMA RAMAN

TRISHNA AGRAWALLA

LEXTECH-CENTRE FOR LAW, ENTREPRENEURSHIP AND INNOVATION

CONTACT US:

INSTRAGRAM LINKEDIN EMAIL